GUIDE PRATIQUE SPST

SERVICES DE PRÉVENTION ET DE SANTÉ AU TRAVAIL

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

TABLE DES MATIÈRES

INTRODUCTION

Les services de prévention et de santé au travail (SPST) ont pour mission principale d'éviter toute altération de l'état de santé des travailleurs du fait de leur travail et en particulier de conduire des actions de santé au travail, de prévenir les risques professionnels, d'assurer le suivi individuel de l'état de santé de chaque travailleur.

Selon l'effectif de l'entreprise, de l'établissement ou du groupe, le SPST peut être organisé :

- soit en service interentreprises, organisme à but non lucratif (association loi 1901) doté de la personnalité morale (plus rarement groupement d'intérêt économique), auquel l'employeur adhère ;
- soit en service autonome administré par l'employeur, au sein du groupe, de l'entreprise ou de l'un de ses établissements.

Le fonctionnement du SPST, doté ou non de la personnalité morale, repose sur différentes catégories de professionnels (dont le régime est organisé par principalement par le code du travail). Ainsi, qu'il soit interentreprises ou autonome, le SPST est composé d'une pluralité d'acteurs pour garantir son bon fonctionnement tant médical qu'administratif :

- membres de l'équipe pluridisciplinaire de santé au travail :
  - > professionnels de santé visés par le code du travail et/ou répondant aux conditions d'exercice prévues par le code de la santé publique : médecins du travail qui animent et coordonnent l'équipe, collaborateurs médecins (médecins en reconversion), médecins praticiens correspondants, internes en médecine du travail, infirmiers en santé au travail, étudiants en médecine ou en soins (p. ex. : externes, infirmiers) ;
  - > autres professionnels tels que toxicologues, ergonomes, hygiénistes, épidémiologistes, statisticiens, assistants de service de santé au travail, etc. ;
- personnels de direction : directeurs, sous-directeurs, adjoints, etc. ;
- personnels administratifs : personnels en charge des adhésions, de la gestion des ressources humaines, agents comptables pour le SPST interentreprises, personnels du service informatique, personnels du service juridique, etc.

Si le SPST peut également intégrer un service social, les travailleurs sociaux y exerçant ne sont en revanche pas considérés comme des membres de l'équipe pluridisciplinaire.

Chacun de ces professionnels composant le SPST contribue à son bon fonctionnement, dans le respect de ses missions et des règles déontologiques qui lui sont éventuellement applicables.

Selon leurs compétences et la nature des missions exercées, les professionnels exerçant au sein d'un SPST peuvent être amenés à collecter, recevoir ou transmettre des informations sur des travailleurs afin d'assurer le suivi de leur état de santé ou de répondre aux obligations assignées aux SPST (p. ex. : tenue du dossier médical en santé au travail, rédaction de la fiche d'entreprise).

Les professionnels des SPST interentreprises traitent également des informations portant sur d'autres personnes que les travailleurs dont ils assurent le suivi. Il peut s'agir de :

- leurs propres personnels au titre de la gestion des ressources humaines, du recrutement, etc. ;
- leurs fournisseurs ;
- des représentants de leurs adhérents s'agissant des SPST interentreprises constitués en association ;
- des membres bénévoles des SPST interentreprises constitués en association (siégeant au conseil d'administration et à la commission de contrôle).

Dans tous les cas, tous les professionnels des SPST traitent les informations obtenues dans le cadre de leur activité professionnelle pour le compte du SPST au sein duquel ils exercent.

Que ces données soient informatisées ou contenues dans un document papier, elles constituent des informations personnelles, qualifiées juridiquement de « données à caractère personnel ». Elles sont donc soumises à la réglementation sur la protection des données et, pour certaines d'entre elles, sont également couvertes par le secret professionnel qui s'impose à tout professionnel de santé.

Attention

Le présent guide s'adresse à l'ensemble des professionnels intervenant au sein du SPST, tant les professionnels de l'équipe pluridisciplinaire de santé au travail que le personnel administratif et de direction, ce dernier étant plus particulièrement en charge de démontrer la conformité aux règles Informatique et Libertés et de garantir leur respect.

NOTIONS CLÉS

Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est une information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement.

Par exemple, il peut s'agir d'informations sur :

- l'identification du travailleur (p. ex.: nom, prénom, service), sa vie professionnelle (p. ex.: relations entretenues avec ses collègues, informations relatives à sa hiérarchie), sa santé (p. ex.: pathologie, état psychologique, soins, arrêt maladie) ;
- les personnes référentes au sein des entreprises, les salariés pour les SPST interentreprises.

Attention

Une information, qui ne permet a priori pas d'identifier le travailleur, peut être une donnée personnelle si, associée à d'autres informations, elle permet à quiconque d'identifier indirectement la personne (p. ex. : le nom de l'employeur du travailleur combiné à une durée d'arrêt maladie permet d'identifier le travailleur en question).

En pratique, certaines de ces informations peuvent figurer sur divers types de supports (p. ex. : dossier médical en santé au travail, courrier d'alerte adressé à l'employeur, bases de données relatives aux adhérents ou aux salariés pour les SPST interentreprises).

Qu'est-ce qu'un traitement de données personnelles ?

La notion de traitement désigne **toute utilisation de données personnelles** : collecte, enregistrement, organisation, structuration, conservation, consultation, utilisation ou encore destruction de telles données.

Dans le cadre de leurs activités au sein des SPST, les professionnels sont amenés à consulter, à utiliser, à conserver et, au bout d'un certain temps, à détruire, des données personnelles concernant les travailleurs et, pour les SPST interentreprises, d'autres catégories de personnes (notamment salariés, adhérents).

Pourquoi et comment protéger les données personnelles ?

La réglementation relative à la protection des données personnelles (règlement général sur la protection des données (RGPD) et loi Informatique et Libertés) a vocation à protéger les informations relatives à la vie privée des citoyens, qu'elles soient d'ordre professionnel ou personnel. Ainsi, même les informations collectées dans un contexte professionnel sont protégées par la réglementation.

Cela signifie que lorsqu'un organisme comme un SPST manipule des informations relatives à des personnes physiques, il doit veiller à respecter certains principes afin de ne pas porter atteinte à leurs droits à la vie privée et à la protection de leurs données personnelles.

Parmi ces garanties, des mécanismes doivent être mis en œuvre permettant tout à la fois d'assurer la confidentialité des informations et de garantir le lien de confiance entre le travailleur et les professionnels de l'équipe pluridisciplinaire du SPST en évitant la divulgation d'informations sensibles, en particulier les données de santé.

Attention

Le respect de la réglementation en matière de protection des données n'exonère pas le SPST du respect des autres obligations auxquelles il est par ailleurs soumis. Les principes du RGPD et de la loi Informatique et Libertés ne doivent en effet pas permettre de déroger à d'autres règles, issues par exemple du code du travail ou du code de la santé publique.

Pour toute interrogation relative à la protection des données personnelles, les membres des SPST autonomes peuvent se rapprocher du délégué à la protection des données de leur organisme (dit DPD, ou, plus couramment, DPO pour *Data protection officer* en anglais) lorsqu'il a été désigné.

Chargé de mettre en œuvre la conformité à cette réglementation, le DPD peut fournir des conseils et accompagner le SPST dans ses démarches de mise en conformité.

POUR ALLER PLUS LOIN

- Articles 3 du RGPD (champ d'application), cnil.fr
- Article 4 du RGPD (définitions), cnil.fr
- Article 37 du RGPD (désignation d'un délégué à la protection des données), cnil.fr

QUESTIONS COMMUNES AUX DIFFÉRENTS FICHIERS CONSTITUÉS PAR LES SPST

FICHE N° 1 : POUR QUELLES FINALITÉS (OBJECTIFS) LE SPST PEUT-IL UTILISER DES DONNÉES PERSONNELLES ?

Règles de droit

Le SPST représenté par sa direction, lorsqu'il est responsable de traitement d'un fichier ou d'une base de données, doit identifier la raison pour laquelle il souhaite utiliser des données personnelles. Il s'agit **d'identifier l'objectif poursuivi** par l'utilisation de ces données en définissant précisément ce à quoi le fichier doit servir, et **ce avant de commencer à utiliser les données relatives** à un travailleur, à un adhérent du SPST interentreprises, ou à toute autre personne (salariés du SPST interentreprises, représentants des employeurs au conseil d'administration du SPST interentreprises, etc.).

Les professionnels du SPST ne doivent en effet recueillir des données personnelles, notamment sur les travailleurs (p. ex. : informations de santé, conditions d'exercice de l'activité professionnelle telles que les horaires, le statut du travailleur, l'organisation de l'équipe, l'exposition à certains risques) que pour des finalités **déterminées, explicites et légitimes**.

L'objectif poursuivi par l'utilisation des données personnelles doit être défini en amont

La détermination de l'objectif poursuivi par le SPST doit toujours être réalisée **avant l'utilisation des données relatives aux personnes concernées** (travailleurs, professionnels du SPST, adhérents, etc.). Cet objectif permet de :

- **déterminer la nature et l'étendue des données collectées par les différents services du SPST** (équipe pluridisciplinaire, service administratif en charge de la gestion des adhésions dans un SPST interentreprises, comptabilité, direction, etc.), ainsi que le **moment de la collecte**. Seules les données adéquates et strictement nécessaires pour atteindre l'objectif invoqué pourront être collectées ;
- **définir les durées de conservation des données collectées :** en fonction de la finalité du fichier et de l'éventuelle existence d'une réglementation imposant une durée de conservation déterminée, les données collectées pourront être conservées plus ou moins longtemps. Par exemple, une durée de conservation distincte sera utilisée pour le dossier médical en santé au travail (DMST) et pour le fichier utilisé dans le cadre d'une recherche menée sur les troubles musculo-squelettiques ou encore pour le fichier utilisé, au plan des ressources humaines, pour la gestion des salariés du SPST interentreprises.

› Pour plus d'informations sur la durée de conservation des données, voir la fiche n° 5 et la fiche n° 10.
L'objectif fixé pour l'utilisation des données personnelles doit être respecté tout au long de leur utilisation.

L'objectif poursuivi doit être déterminé

L'objectif de la collecte des données personnelles doit être défini avec suffisamment de précision. Il ne doit pas y avoir de buts cachés, ni de collecte de données « au cas où » qui pourraient être utiles à des objectifs non encore définis.

Exemples

Concernant l'utilisation des données personnelles ayant pour objectif la réalisation d'études et d'enquêtes, s'il est indiqué aux travailleurs que ce « traitement est mis en œuvre à des fins d'intérêt légitime », il ne s'agit pas d'un objectif déterminé puisqu'il ne permet pas de comprendre l'objectif poursuivi (en l'occurrence, la réalisation d'études et d'enquêtes dans un domaine particulier).

De même, lorsque les professionnels du SPST collectent des informations relatives à des personnes extérieures au service (personnes « contacts » au sein des entreprises adhérentes, fournisseurs, tiers, etc.), ils doivent connaître les raisons concrètes pour lesquelles ils le font.

L'objectif poursuivi doit être explicite

Dès lors que les professionnels du SPST utilisent des données personnelles, l'objectif poursuivi doit être énoncé en **des termes clairs, simples et compréhensibles**.

Ainsi, chaque professionnel du SPST **doit être en mesure d'indiquer la raison justifiant la collecte de données des travailleurs** ou des autres personnes concernées par une utilisation de leurs données, quand bien même cet objectif pourrait être considéré comme évident.

L'objet de la collecte des données personnelles doit en effet être **porté à la connaissance des personnes concernées pour leur permettre de comprendre les modalités pratiques d'utilisation de leurs données**. Ces personnes doivent ainsi savoir quelles sont les utilisations possibles de leurs données personnelles par les professionnels du SPST dans le cadre des fichiers et base de données déployés.

Cette description de la finalité de la collecte des données est par ailleurs **nécessaire pour la tenue du registre des activités de traitement** listant les fichiers et les bases de données utilisées par les SPST.

› Pour plus d'informations sur ce registre, voir la fiche n° 9.

Exemples

Si le SPST se contente d'informer les travailleurs que *« des traitements sont mis en œuvre pour l'exercice de ses missions »*, il ne s'agit pas d'un objectif explicitement énoncé puisqu'il ne permet pas aux travailleurs de comprendre l'objectif poursuivi par les traitements constitués.

À l'inverse, si les travailleurs sont informés que les données personnelles sont utilisées par les professionnels du SPST en vue de la rédaction de la fiche d'entreprise recensant les risques professionnels et les effectifs des salariés exposés, l'objectif poursuivi est explicite et permet aux travailleurs de comprendre pour quelles raisons les informations sont utilisées.

De la même façon, les traitements mis en œuvre à des fins de gestion du personnel doivent être définis précisément. Il ne peut être seulement fait mention du fait que ce *« traitement est mis en œuvre à des fins de bon fonctionnement du SPST »*.

L'objectif poursuivi doit être légitime

Au sens de la réglementation sur la protection des données personnelles, **la légitimité de l'objectif poursuivi en créant un fichier s'apprécie par rapport à l'ensemble de la législation applicable au fichier mis en œuvre**. Cet objet du fichier ne sera ainsi pas légitime s'il porte atteinte notamment à une réglementation spécifique (loi, décret, arrêté) ou à une liberté fondamentale.

À l'inverse, **on peut présumer que l'objectif est légitime dès lors que les données personnelles sont utilisées pour répondre à une obligation imposée par une loi ou une réglementation** ou qu'elle correspond aux missions du responsable de traitement, notamment dans le secteur public.

Exemple

Lors d'une restructuration entraînant la suppression de postes, l'élaboration d'une liste nominative des travailleurs identifiés comme « fragiles » par les professionnels du SPST en vue de la transmettre à l'employeur ne peut pas être considérée comme un objectif légitime. Le SPST doit en effet éviter toute altération de la santé des travailleurs du fait de leur travail en respectant les missions définies par le code du travail. La communication d'une telle liste supposerait une violation du secret professionnel par le médecin du travail. Elle correspondrait à la violation cumulée d'un ensemble de textes.

En effet, une **telle pratique n'est pas conforme** à la réglementation relative à la protection des données (le traitement est dans ce cas illicite). Elle est par ailleurs susceptible de constituer une violation d'autres textes relevant notamment du droit du travail, du code pénal et de la déontologie médicale.

En pratique

Au sein d'un SPST, des données personnelles peuvent être collectées pour des raisons multiples. L'utilisation de ces données pourra répondre à des objectifs très spécifiques tels que :

- Gérer le **DMST** : au moment de l'embauche, lors de la visite d'information et de prévention ou de l'examen médical d'aptitude, un DMST est ouvert par le professionnel de santé du SPST. Il retrace, dans le respect du secret médical, les informations relatives à l'état de santé du travailleur, aux expositions auxquelles il a été soumis ainsi que les avis et propositions du médecin du travail (par exemple concernant les mesures individuelles d'aménagement, d'adaptation ou de transformation du poste de travail ou des mesures d'aménagement du temps de travail).

> Pour plus d'informations sur le DMST, nous vous invitons à consulter la fiche n° 10.

- Renseigner le **dossier consacré à l'entreprise** constitué notamment pour rédiger la fiche d'entreprise et mener toutes les actions en lien avec les missions imparties au SPST (conduite des actions en santé au travail, actions menées pour diminuer les risques professionnels, etc.) : le médecin du travail ou les autres membres de l'équipe pluridisciplinaire établissent et mettent à jour une fiche sur laquelle figurent notamment les risques professionnels et les effectifs des travailleurs qui y sont exposés. La fiche d'entreprise, même si elle ne contient aucune donnée directement identifiante, est susceptible de contenir des données personnelles pseudonymisées des travailleurs concernés (notamment via la mention des effectifs des salariés exposés à des risques professionnels identifiés dans une entreprise déterminée et lorsque peu de salariés sont concernés par cette exposition : dans une telle situation, l'anonymat des travailleurs concernés pourrait ne pas être assuré).
- Gérer, au plan des ressources humaines, les **salariés du SPST** : les SPST interentreprises disposent de leurs propres salariés pour fonctionner, ce qui implique l'utilisation de données personnelles.

> Pour plus d'information sur les traitements de données utilisés pour gérer les salariés, nous vous invitons à consulter le référentiel relatif à la gestion des ressources humaines de la CNIL.

- **Assurer l'administration du SPST** telle que l'organisation des instances, la gestion des relations avec le comité économique et social, etc.
- **Réaliser des recherches, études et enquêtes** : le médecin du travail participe, notamment en liaison avec le médecin inspecteur du travail, à toutes recherches, études et enquêtes, en particulier à caractère épidémiologique, entrant dans le cadre de ses missions. Il peut, à ce titre, réutiliser les données personnelles figurant dans le DMST.

> Pour plus d'informations sur les recherches, études et enquêtes, voir la fiche n° 12.

> Pour plus d'informations sur les finalités des traitements constitués par les SPST, voir l'annexe n° 1.

Les données recueillies sur les travailleurs par les SPST (par exemple à l'occasion des visites d'information et de prévention, de pré-reprise et de reprise du travail, etc.) et qui sont inscrites dans le DMST - notamment les informations de santé et celles en lien avec leurs conditions de travail - seront très **souvent réutilisées** par les professionnels de santé du SPST pour répondre à l'exercice des missions du service telles que le suivi et la traçabilité des expositions professionnelles ou encore la veille sanitaire. Des données personnelles à caractère administratif peuvent également être réutilisées notamment aux fins d'établir les rapports de branche.

> Pour plus d'informations sur les conditions de réutilisation des données, nous vous invitons à consulter l'annexe n° 2.

Les questions à se poser

- L'objectif poursuivi par l'utilisation des données personnelles du fichier est-il **déterminé, explicite et légitime** ?
- Les données recueillies sur les travailleurs pour répondre à cet objectif **sont-elles réutilisées pour répondre à un autre but (p. ex. : la recherche)** ? Si oui, une analyse de compatibilité a-t-elle été réalisée ?
- La **démarche de conformité** a-t-elle été **documentée** ?

POUR ALLER PLUS LOIN

- Article 5 du RGPD (principes), cnil.fr
- Article 6.4 du RGPD (licéité du traitement), cnil.fr
- Articles L. 4624-8, R. 4624-45-3 et suivants, et R. 4624-46 du code du travail (dossier médical en santé au travail et risques professionnels), legifrance.gouv.fr

FICHE N° 2 : QUI EST RESPONSABLE DE TRAITEMENT DES DONNÉES PERSONNELLES UTILISÉES PAR LE SPST ?

Règles de droit

La réglementation en matière de protection des données personnelles non seulement précise la manière dont les informations doivent être utilisées, mais également désigne la personne qui doit concrètement assumer la responsabilité de la bonne application de ces règles.

Le RGPD prévoit ainsi trois statuts possibles pour les acteurs : **responsable de traitement, responsable conjoint et sous-traitant** :

- Le **responsable de traitement** est la personne morale ou le service qui détermine l'objectif poursuivi par l'utilisation qui est faite des informations et les modalités concrètes d'utilisation (p. ex.: nature des informations collectées, durée de conservation des informations, mesures de sécurité mises en place, détermination de la politique de gestion des habilitations et des accès). Il détermine ainsi les modalités d'utilisation et est, à ce titre, responsable du bon respect des règles. Le responsable de traitement porte ainsi l'entière responsabilité de la conformité du traitement aux règles Informatique et Libertés. À noter que la responsabilité de traitement se distingue ainsi de la responsabilité juridique.
- Dans d'autres situations, plusieurs personnes ou services peuvent décider conjointement de l'objectif et des modalités pratiques d'utilisation des données personnelles : on parle alors de **responsables conjoints des données**. Dans le cas d'une responsabilité conjointe, un accord doit être conclu afin de définir de manière transparente le rôle et les obligations respectives de chacun en ce qui concerne le respect des règles issues du RGPD, sauf à ce que ces obligations aient été définies par le droit de l'Union ou de l'État membre auquel les responsables conjoints sont soumis.
- Parfois, le responsable de traitement peut faire appel à un organisme pour manipuler des informations pour son propre compte, sur son instruction et sous son autorité : cet organisme est alors considéré comme un **sous-traitant** au sens du RGPD.
  Un contrat ou un autre acte juridique devra être établi. Il précisera les obligations du responsable de traitement et du sous-traitant en ce qui concerne notamment l'objet, la durée, la nature et l'objectif de l'utilisation des informations ou encore les catégories d'informations collectées sur les travailleurs.

En pratique

Comment déterminer le responsable des traitements utilisés par le SPST ?

Les SPST sont susceptibles de prendre différentes formes : service autonome propre à l'entreprise, service interentreprises, service intégré au sein d'une caisse de mutualité sociale agricole (MSA) pour le régime agricole, etc.

En raison de leur **caractère polymorphe**, des **diverses modalités de fonctionnement** et de la **variété des fichiers** pouvant être mis en œuvre, le partage de la responsabilité dans la collecte des données personnelles peut être différent d'un SPST à un autre et/ou d'un fichier à un autre.

Attention

La ligne de partage entre ces trois catégories peut parfois être délicate à fixer. La qualification doit intervenir au terme d'une **analyse concrète des modalités de création et de mise en œuvre du fichier ou de la base de données constitué au niveau du SPST**.

Selon la logique de responsabilisation, il appartient à chaque acteur (notamment SPST, employeurs, comité social et économique) de documenter l'analyse ayant conduit à telle ou telle qualification retenue. Attention, **cela ne signifie pas que chacun peut « choisir » la qualification qui l'arrange, la qualification devant refléter la réalité**. En cas de doute, il est important de **documenter la réflexion qui a été menée** pour aboutir à cette qualification et d'être en mesure de la justifier.

La définition des responsabilités permet uniquement de définir aisément les obligations de chacune des parties. Une répartition erronée des responsabilités n'emporte donc pas de grandes conséquences si les obligations relatives à la protection des données ont été respectées.

Nature des obligations	Articles RGPD	Responsable de traitement	Sous-traitant	Responsable conjoint
Rédiger un écrit précisant les obligations respectives de chacun des acteurs	26 ; 28	✓	✓	✓
Documenter les instructions du responsable de traitement concernant les fichiers exploités par le sous-traitant		✓	✓	✓
Obtenir et conserver une autorisation écrite préalable du responsable de traitement pour recourir aux services d'un sous-traitant	28	✗	✓	✗
Tenir un registre des activités de traitement	30	✓	✓	✓
Réaliser une analyse d'impact (si les critères du RGPD sont réunis)	35	✓	✗	✓
Informer les co-contractants (responsable de traitement, sous-traitant, co-responsable) en cas de soupçon de violation du RGPD	28	✗	✓	✗
Informer la CNIL et/ou les personnes concernées en cas de violation des données	33 ; 34	✓	✗	✓
Fournir aux personnes concernées les informations obligatoires	12 à 14	✓	✗	✓
Traiter les demandes d'exercice de droits (accès, effacement, opposition, etc.)	15 à 23	✓	✗	✓
Assister le responsable de traitement dans la gestion de demandes d'exercice des droits	28	Sans objet	✓	✗

Le **partage des responsabilités entre les différentes parties prenantes doit être évalué, au cas par cas, pour identifier celui qui dispose d'un pouvoir décisionnel sur le fichier**, en prenant en compte les différents éléments suivants :

- Qui est obligé (si la création du fichier est obligatoire) ou qui souhaite que les données personnelles soient utilisées dans un but particulier ?
- À qui revient le choix final de l'outil « métier » permettant d'utiliser et d'organiser les données personnelles ?
- Qui définit les modalités d'utilisation des données personnelles (durée de conservation, destinataires à qui sont communiquées les données, mesures de sécurité, etc.) ?

Qui est responsable du traitement constitué pour gérer les dossiers médicaux en santé au travail (DMST) ?

Un SPST est toujours responsable de traitement pour le fichier utilisé dans le cadre de la gestion des DMST (que le SPST soit autonome ou interentreprises). Le code du travail le désigne en effet expressément comme tel. Il précise également les caractéristiques essentiel du traitement (notamment finalité du DLMST, nature des données collectées, destinataires, durée de conservation).

De ce fait, il incombe, en pratique, au SPST et plus particulièrement à sa direction, de veiller au respect du régime juridique qui découle de cette responsabilité de traitement. Ainsi, le SPST représenté par sa direction doit garantir la bonne utilisation des données du DMST, notamment leur conservation pour une durée conforme à la réglementation, la possibilité de restreindre les accès conformément aux compétences et missions exercées par chacun des professionnels du SPST et aux règles de confidentialité, la mise en œuvre de mesures de sécurité adéquates, le cas échéant le recours à un hébergeur de données de santé certifié (ou agréé selon la réglementation applicable), etc.

La direction du SPST doit mettre à disposition des professionnels de santé (notamment infirmiers, médecins du travail, internes en médecine du travail) et des autres membres de l'équipe pluridisciplinaire (tels que les toxicologues, ergonomes, kinésithérapeutes, statisticiens ou épidémiologistes) une organisation et des moyens adaptés, pour assurer le respect des obligations en matière de protection des données personnelles. À cet égard, elle doit être particulièrement vigilante dans le choix de la solution logicielle utilisée pour gérer le DMST.

Attention

D'après les lignes directrices du Comité européen de la protection des données sur les notions de responsable de traitement et de sous-traitant dans le RGPD, adoptées le 7 juillet 2021, c'est généralement l'organisation en tant que telle, et non une personne au sein de celle-ci, qui agit en tant que responsable de traitement au sens du RGPD. Même si une personne physique particulière est désignée pour veiller au respect des règles en matière de protection des données, cette personne ne deviendra pas pour autant le responsable du traitement mais agira pour le compte de l'entité juridique qui, en sa qualité de responsable de traitement, sera responsable en dernier ressort en cas de violation des règles.

Décliné au SPST, il apparaît clairement que la **responsabilité professionnelle et la responsabilité de traitement se réfèrent à deux notions distinctes**. Si le médecin du travail dispose de l'indépendance professionnelle et qu'il est explicitement visé comme le responsable de la constitution du DMST, il agit dans un environnement, pour partie contraint par les dispositions du code du travail, et pour le compte d'un collectif organisé par une direction. Il revient par ailleurs au SPST, et plus particulièrement à la direction du service, de veiller au respect de la conformité des fichiers et bases de données déployés au sein des SPST aux dispositions issues du RGPD et de la loi Informatique et Libertés.

Par exemple, pour le traitement relatif à la gestion du DMST, la direction du SPST doit s'assurer qu'une analyse d'impact relative à la protection des données est réalisée, que la fiche du registre des activités de traitement est établie, qu'un contrat a bien été passé avec l'éventuel sous-traitant, que des mesures de sécurité telles que l'utilisation d'antivirus et la restriction des accès physiques au locaux et aux données contenues dans le DMST sont bien définies, et que la durée de conservation du DMST est respectueuse des dispositions du code du travail. Au regard de ces éléments, il apparaît que le SPST est responsable de traitement, au même titre que les établissements de santé pour les dossiers des patients.

Même si le SPST, représenté par sa direction, est responsable du traitement concernant la gestion du DMST, certaines garanties existent pour les professionnels de santé y exerçant :

- concernant le **choix de la solution logicielle utilisée pour le DMST**, le Conseil national de l'ordre des médecins (CNOM) considère que celui-ci doit être décidé en accord avec le médecin utilisateur ou son représentant et ne peut relever du seul choix de l'employeur (rapport du CNOM, le dossier médical en santé au travail, 17 et 18 décembre 2015) ;
- concernant **l'accès aux données du DMST**, les personnels de direction et, plus globalement, les personnels administratifs ne sont pas autorisés à en prendre connaissance. Il est ainsi prévu dans le code du travail que seuls les professionnels de santé et certains autres membres de l'équipe pluridisciplinaire, placés sous la supervision du médecin du travail, peuvent consulter et alimenter le DMST dans le respect du secret médical (article L.4624-8 du code du travail). Les niveaux d'accès des membres de l'équipe pluridisciplinaire sont limités à certaines catégories de données ; la Haute Autorité de santé (HAS) recommande par ailleurs que la gestion des accès soit assurée par le médecin du travail administrateur du logiciel ;
- concernant la pratique professionnelle, le médecin du travail est soumis à des **règles déontologiques particulières** : il continue donc à exercer ses missions de manière indépendante. Par exemple, pour chacun des travailleurs dont il assure le suivi individuel, il est seul compétent pour apprécier la pertinence des informations qu'il souhaite voir figurer dans le DMST pour garantir ce suivi, conformément aux articles R. 4624-45-3 et suivants du code du travail. Au quotidien, il est le **garant du respect des règles de confidentialité applicables au DMST** qu'il supervise au plan opérationnel.

Qui est responsable de traitement lorsque des données personnelles sont utilisées par le SPST pour mener des recherches, études et enquêtes ?

Le SPST est en principe responsable de la collecte des données et de leur utilisation pour les recherches, études et enquêtes qui sont internes.

Une recherche, étude ou enquête est interne dès lors qu'elle répond à ces conditions cumulatives :

- elle est réalisée **pour le compte du SPST et pour son usage exclusif** ;
- elle est réalisée à partir **des informations figurant dans les DMST des travailleurs que le SPST suit**.

En pratique, les recherches, études et enquêtes sont menées par les médecins du travail ou sous leur responsabilité. Elles permettent de fournir des indicateurs en santé au travail, d'identifier des affections pouvant être provoquées ou aggravées par une activité professionnelle spécifique ou encore de déterminer les actions de santé au travail à mettre en œuvre pour préserver la santé physique et mentale des travailleurs dans une entreprise donnée et de répondre ainsi aux missions légalement dévolues au SPST.

Attention

Même si le SPST **est en principe responsable de la collecte des données et de leur utilisation pour les recherches, études et enquêtes** qui sont internes, la décision du déclenchement d'une recherche, d'une étude ou d'une enquête interne et sa méthodologie (choix des données à collecter, personnes concernées, durées de conservation, destinataires, etc.) relève uniquement du médecin du travail. Il convient ainsi de **distinguer la responsabilité opérationnelle de conduite de la recherche, étude ou enquête et la responsabilité juridique** associée à la création du traitement de données personnelles (en l'occurrence un fichier ou une base de données) constitué pour la mener.

Les recherches, études ou enquêtes sont menées au sein d'une structure organisée, à savoir le SPST, pour répondre à ses missions définies par l'article L. 4622-1 du code du travail. Le médecin, bien qu'il dispose d'une indépendance professionnelle, agit pour le compte du SPST. En conséquence, c'est bien le SPST qui endosse la responsabilité juridique du traitement nécessaire à l'exercice de ses missions.

En revanche, lorsque la recherche, l'étude ou l'enquête est multicentrique ou implique que des données personnelles soient rendues accessibles à des personnes extérieures à l'équipe du SPST (p. ex. : organisation d'une étude nécessitant la consultation des DMST des travailleurs d'une même région par les spécialistes d'une pathologie particulière exerçant au sein d'un centre hospitalier universitaire (CHU)), il conviendra d'examiner au cas par cas qui est responsable de la collecte des données personnelles et des modalités d'utilisation pour identifier le responsable ou, le cas échéant, les responsables du traitement.

Qui est responsable des traitements utilisés pour d'autres objectifs que la gestion du DMST et les recherches, études et enquêtes (ex : gestion des adhérents du SPST, gestion des salariés exerçant au SPST) ?

DANS UN SPST AUTONOME

Scénario n° 1 : le SPST peut être responsable des traitements

Un SPST autonome est responsable de traitement dès lors qu'il définit, **sans que l'employeur intervienne** :

- les raisons le poussant à utiliser des données personnelles, c'est-à-dire son objectif ;
- les modalités d'utilisation des données (nature des informations collectées, durée de conservation des informations recueillies, mesures de sécurité, etc.).

> **Exemple**
>
> Le SPST est en principe responsable de traitement pour la gestion et l'organisation des visites de suivi des travailleurs.

Lorsque le SPST autonome est responsable de traitement, l'employeur doit mettre à sa disposition les moyens humains et financiers permettant d'assurer la conformité des fichiers aux règles relatives à la protection des données.

L'employeur, en tant que personne morale de rattachement, assume d'ailleurs juridiquement les conséquences d'une non-conformité des fichiers mis en œuvre dans un SPST autonome. Cela signifie que l'employeur devra répondre d'éventuels manquements aux principes Informatique et Libertés.

Scénario n° 2 : l'employeur est responsable de certains traitements utilisés par le SPST lorsque ces derniers sont mis en œuvre par le SPST

En fonction de son degré d'implication dans l'utilisation des données personnelles, l'employeur peut être considéré comme responsable du traitement.

> **Exemple**
>
> Il en sera ainsi lorsque l'employeur décide que le SPST doit utiliser des données personnelles pour un objectif que l'employeur a également défini, par exemple l'utilisation des données personnelles des salariés du SPST pour l'organisation des plannings des différents membres du personnel du SPST autonome.

Scénario n°3 : l'employeur et le SPST peuvent être conjointement responsables de certains traitements

Dès lors que chacun des deux est impliqué dans la définition de l'objectif et des modalités d'utilisation des données personnelles, l'employeur et le SPST peuvent être considérés comme des responsables conjoints des fichiers. Cela suppose que l'employeur et le SPST coopèrent réellement pour décider de l'utilisation des informations. Les rôles de chacun des responsables conjoints de traitement devront être précisés dans un accord.

> **Exemple**
>
> L'employeur et le SPST sont en principe responsables conjoints de traitements lorsqu'ils organisent ensemble un événement de prévention tel que des actions en milieu de travail.

DANS UN SPST INTERENTREPRISES

Un SPST interentreprises est un **organisme indépendant** (le plus souvent une association), **administré par un conseil d'administration et disposant d'un budget propre**. Cela signifie qu'il est libre de définir ses modalités de fonctionnement (recrutement, choix des outils utilisés, etc.).

La commission médico-technique, interne au SPST interentreprises, est d'ailleurs en charge de formuler des propositions au conseil d'administration sur les actions menées en son sein notamment en ce qui concerne l'organisation des actions en milieu de travail et du suivi de l'état de santé des travailleurs.
En conséquence, le SPST interentreprises est libre de définir les objectifs et les modalités pratiques de l'utilisation de données personnelles dans le cadre de ses missions habituelles. Il peut donc, sauf exceptions, être considéré comme **responsable de traitement pour toutes les utilisations de données personnelles effectuées par les personnes travaillant en son sein.** Il est considéré comme sous-traitant lorsqu'il exécute une commande effectuée par un autre organisme (cf infra).

Attention

Le SPST interentreprises est responsable de traitement pour tous les fichiers relatifs à la gestion de la structure (recrutement des professionnels du SPST, gestion des prestataires extérieurs, suivi financier et budgétaire, gestion des adhésions, suivi de la comptabilité, etc.).

Dans quels cas le SPST peut-il être sous-traitant ?

Un SPST agit en tant que sous-traitant dès lors qu'il utilise des informations à la demande d'une autre entité.

Exemple

Si un comité social et économique (CSE) fait appel, dans le cadre de ses travaux, à l'expertise du SPST pour réaliser une enquête portant sur les maladies professionnelles dans une entreprise déterminée, le CSE est alors le responsable de traitement. En effet, l'objectif exact de l'enquête, sa méthodologie et ses modalités de mise en œuvre sont en principe définies par le CSE. Dans cette configuration, le SPST est alors le sous-traitant car il agit, sous la responsabilité du CSE, en appliquant strictement ses consignes pour la collecte des données personnelles nécessaires à la réalisation de l'enquête.

De la même façon, s'agissant des intermittents du spectacle, le service de santé spécifique chargé de leur suivi (Thalie santé) peut le confier aux SPST de la région de travail des intermittents, conformément à l'accord national de branche. Dans cette situation, et sous réserve du contenu de la convention liant les deux organismes, le SPST régional est susceptible d'endosser le rôle de sous-traitant de Thalie santé.

Attention

Même lorsqu'un autre organisme agit comme responsable de traitement, le médecin du travail reste soumis à des obligations de confidentialité et ne peut pas divulguer des informations protégées par le secret professionnel.

Il en va de même pour les personnes qui l'assistent dans son exercice, c'est-à-dire les autres membres de l'équipe pluridisciplinaire (p. ex. : ergonomes, kinésithérapeutes, assistants du SPST). Le médecin du travail doit d'ailleurs veiller à les informer de leurs obligations en matière de secret professionnel, conformément à l'article R. 4127-72 du code de la santé publique.

Par conséquent, lorsque le SPST est sous-traitant et que la responsabilité du traitement est endossée par un organisme tiers, le médecin du travail, et plus globalement l'ensemble du personnel du SPST, doivent être particulièrement vigilant en :

- signalant toute mesure prise ou toute situation susceptible de ne pas être conforme aux règles entourant le secret professionnel, par exemple si l'employeur accède aux dossiers médicaux en santé au travail ;
- veillant quotidiennement au strict respect des mesures prises, par exemple en ne communiquant pas un mot de passe personnel à d'autres personnes.

Un SPST peut-il recourir à un sous-traitant pour traiter les données personnelles qu'il utilise pour fonctionner et exercer ses missions ?

Le SPST peut, lorsqu'il est responsable de traitement, décider de recourir à un autre organisme pour l'aider à assurer ses missions.

Si les activités effectuées par cet organisme tiers sont susceptibles de nécessiter la manipulation de données personnelles sous la responsabilité de SPST (p. ex. : hébergement des données du DMST, réorganisation d'un SPST en faisant appel à une société de conseil, gestion administrative, gestion comptable, gestion de la paie), il sera considéré comme un **sous-traitant**, agissant **pour le compte du SPST**.

Ce sous-traitant, qui est également soumis aux obligations relatives à la protection des données, ne peut traiter ces dernières que sur instruction du responsable de traitement.

Attention

Dans certains cas, le sous-traitant peut être soumis à des obligations particulières. Par exemple, si le stockage des DMST des travailleurs est confié à un prestataire chargé d'en assurer la conservation, dans des serveurs à distance, celui-ci doit être **hébergeur certifié** (ou agréé selon la réglementation applicable) pour l'hébergement, le stockage et la conservation des données de santé.

Il appartient au SPST, en tant que responsable de traitement, **d'encadrer la relation de sous-traitance** afin que les données personnelles ne soient ni divulguées, ni modifiées ou supprimées par inadvertance ou malveillance. Un contrat clair doit ainsi être établi afin de préciser les obligations de chacune des parties prenantes et se conformer à la réglementation.

Les mentions devant figurer dans le contrat de sous-traitance sont énoncées à l'article 28 du RGPD.

Le contrat doit au moins mentionner :

- les actions confiées au sous-traitant (p. ex. : quelles opérations doit-il effectuer sur les données ? Que doit-il faire des informations à la fin de la relation ?) ;
- la nécessité de demander l'autorisation écrite si le sous-traitant souhaite faire appel lui-même à un autre sous-traitant ;
- la mise à disposition par le sous-traitant de toutes les données nécessaires pour démontrer le respect des obligations.

Plus globalement, le SPST est invité à préciser les obligations de chacune des parties dès lors qu'il existe une transmission d'informations.

Lorsque le SPST est assuré par un organisme externe à l'établissement employant les travailleurs bénéficiaires de ce service (SPST interentreprises), il est conseillé aux deux parties (employeurs et SPST interentreprises) de préciser les **responsabilités de chacune d'elles** dans le contrat les liant et d'indiquer les obligations qui en découlent, notamment concernant la protection des données personnelles des travailleurs.

Attention

Pour encadrer les rôles et obligations, le SPST peut utilement se rapprocher du délégué à la protection des données de son organisme afin d'être aidé pour la réalisation du contrat.

> Pour obtenir davantage de précisions, vous pouvez prendre connaissance du guide pratique de la CNIL sur la sous-traitance afin de comprendre vos droits et obligations.

Les questions à se poser

Les SPST devront, pour identifier le statut exact des différents acteurs (notamment employeurs, CSE, prestataires extérieurs), **se poser les questions suivantes** :

- Qui décide de mettre en œuvre la collecte des données personnelles ?
- Qui définit les caractéristiques du fichier utilisé pour la collecte des informations telles que la nature des données personnelles recueillies, les durées de conservation, ou encore l'outil choisi ?
- Les relations entre les différentes parties prenantes sont-elles bien encadrées (contrat établi entre le sous-traitant et le responsable de traitement ou convention entre les différents co-responsables de cette collecte) ?
- En cas de sous-traitance, le sous-traitant respecte-t-il les obligations découlant des textes ?
- La réflexion conduisant à retenir telle ou telle qualification a-t-elle bien été documentée ?

POUR ALLER PLUS LOIN

- Articles 4 du RGPD (définitions), cnil.fr
- Article 24 du RGPD (responsabilités du responsable de traitement), cnil.fr
- Articles L. 4622-4 et suivants du code du travail (services de prévention et de santé au travail), legifrance.gouv.fr
- Article L. 2315-94 du code du travail (appel à un expert habilité par le conseil social et économique), legifrance.gouv.fr
- Article R.4624-45-3 du code du travail (dossier médical en santé), legifrance.gouv.fr
- Article L. 1111-8 du code de la santé publique (hébergement de données de santé), legifrance.gouv.fr
- Article R. 4127-96 du code de la santé publique (conservation des dossiers médicaux), legifrance.gouv.fr
- Lignes directrices du Comité européen de la protection des données concernant les notions de responsable de traitement et de sous-traitant dans le RGPD, 7 juillet 2021 (PDF, 1,6 Mo), edpb.europa.eu

FICHE N° 3 : QUELLES DONNÉES PEUVENT ÊTRE COLLECTÉES PAR LE SPST ?

Règles de droit

Les professionnels du SPST doivent veiller à ne traiter que les informations **adéquates, pertinentes et limitées à ce qui est nécessaire** au regard de l'objectif poursuivi (principe de minimisation). C'est la raison pour laquelle il est essentiel de définir l'objectif de l'utilisation des données personnelles avec suffisamment de précision pour identifier quelles sont les données que le SPST peut collecter et utiliser.

• **Les données personnelles collectées doivent avoir un lien direct avec l'objectif poursuivi par le fichier.**

Cela signifie que le professionnel doit si besoin faire un tri dans les informations fournies par la personne concernée (travailleur, adhérent du SPST interentreprise, salarié, etc.) afin de ne garder que celles qui lui permettent de remplir ses missions.

• **Les données personnelles utilisées doivent être nécessaires à la poursuite de l'objectif poursuivi.**

Les données personnelles collectées et utilisées doivent être nécessaires, selon l'objectif poursuivi par l'utilisation des données, au suivi médical du travailleur, à la réalisation d'une enquête consacrée aux risques professionnels auxquels les travailleurs d'une entreprise sont exposés, à la gestion du personnel pour le fichier utilisé à cette fin dans un SPST interentreprises, ou encore à l'établissement de la fiche d'entreprise, etc.

Les professionnels des SPST doivent ainsi veiller à limiter le volume d'informations enregistrées ainsi que leur niveau de détail. Il s'agit d'être le moins intrusif possible dans la vie privée des personnes concernées par l'utilisation des données et de ne garder que les informations essentielles et d'un niveau de détail approprié. Les données personnelles collectées doivent ainsi être limitées au minimum.

> **Exemple**
>
> Dans un SPST interentreprises, lors du processus de recrutement d'un collaborateur pour assurer les fonctions d'assistant, les informations demandées doivent avoir pour seule finalité d'apprécier la capacité du candidat à occuper le poste proposé et de mesurer ses aptitudes professionnelles. Il est en principe interdit de lui demander son numéro de sécurité sociale et ses coordonnées bancaires, des informations relatives aux membres de sa famille, etc.

• **Les données personnelles ne doivent pas être collectées « au cas où ».**

Les informations collectées doivent être effectivement nécessaires à l'objectif poursuivi, elles ne peuvent pas être traitées « au cas où ».

Afin de définir les informations nécessaires à la réalisation de l'objectif poursuivi, la **finalité du fichier doit être déterminée en amont de la collecte des informations**, en ce qu'elle permet de déterminer la nature et la précision des informations, ainsi que le moment de la collecte.

Exemple

Dans le cas particulier du DMST, même s'il revient au professionnel de santé d'estimer quelles sont les informations qui permettront d'apprécier la relation entre l'état de santé du salarié et son poste de travail, il convient de souligner que la collecte des informations sur l'état de santé du travailleur doit être en lien avec le suivi de celui-ci et les possibilités suffisamment plausibles d'exposition à un risque professionnel.

Ainsi, alors même que le travailleur ne souffre, au moment d'une visite, d'aucune maladie ou blessure d'origine professionnelle, la collecte de certaines informations peut être pertinente au cas où un incident de santé surviendrait à plus ou moins long terme du fait de l'activité professionnelle ou d'une exposition à un risque particulier. Par ailleurs, la collecte de données en lien avec une campagne de promotion de la santé ou de dépistage est également admise. En revanche, les informations qui ne se rapporteraient à aucun risque identifié ou plausible ou sans lien avec de telles campagnes ne devraient être ni collectées, ni conservées.

Attention

Toutes les informations que le travailleur a pu révéler, dans le cadre des échanges, ne doivent pas nécessairement être intégrées dans son dossier médical en santé au travail. Seules celles qui sont utiles à son suivi et à la poursuite des missions du SPST peuvent être enregistrées et conservées. Toutes demeurent en revanche confidentielles.

En pratique

Une multitude de données personnelles peut être traitée dans un SPST, sous réserve que ces dernières soient toujours **adéquates, pertinentes et limitées à ce qui est nécessaire** au regard de l'objectif poursuivi par le fichier ou la base de données déployée.

Les catégories de données susceptibles d'être collectées et utilisées seront différentes, selon que le traitement est constitué pour :

- gérer le **DMST** (pour plus d'informations sur le DMST, voir la fiche n°10) ;
- réaliser des **recherches, études et enquêtes** (pour plus d'informations sur les recherches, études et enquêtes, voir la fiche n°12) ;
- renseigner le **dossier consacré à l'entreprise** constitué notamment pour rédiger la fiche d'entreprise et mener toutes les actions en lien avec les missions imparties au SPST (conduite des actions en santé au travail, actions menées pour diminuer les risques professionnels, etc.) ;
- gérer, au plan des ressources humaines, les **salariés du SPST interentreprises** (voir le référentiel relatif à la gestion des ressources humaines) ;
- **recruter les salariés** du SPST interentreprises (pour plus d'informations, voir le guide du recrutement) ;
- assurer **l'administration du SPST** telle que la gestion de la base de données des adhérents, l'organisation des instances, la gestion des relations avec le comité économique et social, etc.

Les questions à se poser

- Quelles sont les données vraiment nécessaires pour atteindre l'objectif fixé au fichier ?
- Les données recueillies sont-elles objectives ?
- Est-il possible de donner accès aux personnes concernées aux données détenues sur lui par le SPST ou y a-t-il des commentaires excessifs ?
- Des données sensibles sont-elles recueillies ? Est-ce autorisé et justifié au regard des finalités du fichier ou de la base de données ? Est-il possible de faire autrement ?

POUR ALLER PLUS LOIN

- Article 5 du RGPD (principes), cnil.fr
- Article 9 du RGPD (données sensibles), cnil.fr
- Article 44 de la loi Informatique et Libertés (exceptions à l'interdiction de traiter certaines données sensibles), cnil.fr

FICHE N° 4 : À QUELS ORGANISMES EXTÉRIEURS LE SPST PEUT-IL TRANSMETTRE LES DONNÉES PERSONNELLES COLLECTÉES DANS SES FICHIERS ?

Règles de droit

Les professionnels du SPST sont tenus de prendre toutes précautions utiles pour **préserver la confidentialité et la sécurité des données personnelles contenues dans les différents fichiers ou bases de données** (DMST, fichier des adhérents, fichier utilisé pour assurer la gestion des ressources humaines de ses salariés), notamment en empêchant des personnes non autorisées d'y accéder.

Le respect de ce principe suppose une **définition précise des personnes ou organismes extérieurs pouvant accéder ou obtenir la communication des données personnelles collectées au sein des SPST**, également appelées destinataires.

Pour le cas particulier des données personnelles présentes dans le DMST, ce principe s'articule avec les règles de déontologie s'imposant aux professionnels de santé (médecins, infirmiers, internes en santé au travail) et aux autres membres de l'équipe pluridisciplinaire du SPST (notamment gestionnaires ou assistants de service de santé au travail, ergonomes, toxicologues) en particulier celles relatives au **secret professionnel**.

Attention

Un destinataire est une personne ou un organisme extérieur qui reçoit des données personnelles, au titre de l'exercice de ses missions.

Par exemple, les sous-traitants (tels que l'hébergeur de données de santé assurant la conservation du DMST), sont destinataires des données personnelles des travailleurs présentes dans les dossiers médicaux en santé au travail tenus par les SPST.

En pratique

En fonction du type de données personnelles concernées, deux situations doivent être distinguées.

LA DEMANDE DE COMMUNICATION PORTE SUR DES INFORMATIONS DES TRAVAILLEURS COLLECTÉES LORS DES VISITES MÉDICALES OBLIGATOIRES OU INSCRITES DANS LE DMST

Soumis à une obligation de secret professionnel, **les professionnels de santé** (médecins, infirmiers, internes en santé au travail, collaborateurs médecins) et les autres **membres de l'équipe pluridisciplinaire du SPST ne peuvent communiquer d'informations relatives aux travailleurs** obtenues dans le cadre de leur activité professionnelle, **sauf si la loi prévoit expressément une dérogation** (p. ex. : le médecin inspecteur du travail est autorisé par l'article L. 4624-8 du code du travail à accéder au DMST).

Attention

D'après l'article R. 4127-72 du code de la santé publique, le médecin doit veiller à ce que les personnes qui l'assistent dans son exercice soient instruites de leurs obligations en matière de secret professionnel et s'y conforment.

Exemple

Dans le cadre notamment du suivi individuel renforcé du travailleur, le code du travail contraint le médecin du travail à transmettre à l'employeur, à l'occasion du renouvellement de l'examen médical d'aptitude, l'avis d'aptitude ou d'inaptitude versé au DMST et également remis au travailleur.

Par ailleurs, avant toute communication d'informations relatives à la santé du travailleur, les professionnels de santé et les autres membres de l'équipe pluridisciplinaire du SPST doivent être vigilants à ce que **la transmission ne porte pas une atteinte disproportionnée au droit au respect de la vie privée des travailleurs**.

Pour cela, l'équipe du SPST veille :

- à ce que les données personnelles soient adéquates et pertinentes au regard de l'objectif poursuivi par l'utilisation des informations : dans certaines circonstances, des informations anonymes ou pseudonymisées pourront par exemple être suffisantes pour le destinataire (p. ex. : la transmission de la fiche d'entreprise à **l'employeur conformément au modèle indiqué dans l'arrêté du 29 mai 1989 nécessite uniquement la transmission d'informations anonymisées voire, dans de rares cas, des informations pseudonymisées**) ;
- à alerter l'organisme destinataire des informations sur la nécessité de ne pas mettre en œuvre une utilisation nouvelle des informations qui serait incompatible avec l'objectif ayant conduit à la transmission.

Exemple

Peuvent obtenir communication de certaines données personnelles :

- **l'employeur du travailleur**, notamment pour les propositions d'aménagement de poste formulées par le médecin du travail ;
- **les instances sanitaires compétentes (par exemple, le Groupe d'alerte en santé travail (GAST) en cas d'événements en santé inhabituels**, c'est-à-dire des cas groupés d'une même maladie ou de mêmes symptômes (cancers, malaises, prurit, etc.) ou d'une exposition pouvant avoir un impact sur la santé des travailleurs (relargage de fibres d'amiante suite à l'incendie d'un magasin, émission d'hydrogène sulfuré par des algues en décomposition, etc.).

Attention

Si l'employeur, autorisé par les textes, est légitime à obtenir la communication de certaines informations, l'équipe du SPST doit veiller à ne communiquer que les informations nécessaires. Aussi, elle doit être vigilante quant à la nature et au niveau de détail des informations susceptibles d'être communiquées.

Par exemple, en cas de nécessité d'aménagement de poste pour un travailleur, seules les préconisations formulées par le médecin du travail sont nécessaires à l'employeur et sont, par conséquent, communicables. Les informations relatives à un éventuel diagnostic médical ne peuvent en aucun cas faire l'objet d'une transmission.

LA DEMANDE NE PORTE PAS SUR DES INFORMATIONS RELATIVES AUX TRAVAILLEURS SUIVIS PAR LE SPST

Si la demande d'accès ou de communication porte sur des **données personnelles qui ne sont pas relatives à des travailleurs suivis par le SPST** (salariés du SPST interentreprises, personnes « contacts » dans les entreprises adhérentes, etc.), il est nécessaire de s'assurer de la légitimité de la demande.

Exemple

S'agissant des SPST interentreprises, les entités chargées de l'audit et du contrôle financier de l'organisme employeur peuvent obtenir la communication de certaines informations. De la même manière, les différents prestataires auxquels l'organisme employeur est susceptible de sous-traiter la gestion de certaines activités (restauration collective, vote électronique, archivage des documents, tenue des comptes d'épargne, etc.) peuvent être destinataires de données personnelles.

Le tableau ci-dessous rappelle le raisonnement à tenir dans une telle situation.

Le demandeur est

Une autorité ou un organisme disposant d'un droit à la communication des informations (par exemple la CNIL dans le cadre de son pouvoir de contrôle)

1. **Vérifier le texte** l'autorisant à demander ces informations
2. Analyser la **qualité de l'organisme** et le périmètre des informations demandées
3. Communiquer **uniquement les informations qui doivent l'être** en sécurisant la transmission des données

Un tiers ne disposant pas d'un texte autorisant cette demande

1. Analyser la **légitimité de la demande**. La réutilisation envisagée par l'organisme doit être compatible avec la raison de la collecte des données
2. Effectuer **un tri des informations** afin de ne communiquer que celles qui sont nécessaires à l'objectif poursuivi par l'organisme
3. **Informer les personnes concernées** en leur permettant de **s'opposer à cette transmission**
4. Indiquer dans votre **documentation (fiche de registre, éventuelle AIPD)** ce nouveau destinataire

› Pour rappel, la liste de l'ensemble des destinataires doit figurer dans la fiche de registre des traitements dédiée (voir fiche n° 9).

Les questions à se poser

- La demande de communication vise-t-elle des **informations relatives à la santé du travailleur** ? Si oui, une disposition législative permet-elle de **déroger au secret professionnel** en fournissant les informations à l'interlocuteur ?
- La demande de communication d'informations est-elle **légitime** si elle n'est pas prévue par un texte ?
- Quelles informations apparaissent pertinentes ? Est-il possible de transmettre des **informations anonymisées ou d'un niveau de détail moindre** ?
- Les destinataires sont-ils mentionnés dans la **fiche de registre des activités de traitements dédiée** ?

POUR ALLER PLUS LOIN

- Article 32 du RGPD (sécurité du traitement), cnil.fr
- Article L. 4624-1 du code du travail (suivi de l'état de santé du travailleur), legifrance.gouv.fr
- Articles L. 1110-4 et R.4127-4 du code de la santé publique (secret médical et respect de la vie privée du travailleur), legifrance.gouv.fr
- Guide de la CNIL sur les tiers autorisés – 2020 (PD F, 720 ko), cnil.fr

FICHE N° 5 : QUELLE EST LA DURÉE DE CONSERVATION DES FICHIERS CONSTITUÉS PAR LE SPST (HORS DOSSIER MÉDICAL EN SANTÉ AU TRAVAIL) ?

Règles de droit

Les données personnelles utilisées dans les traitements constitués au sein du service de prévention et de santé au travail (SPST) doivent être conservées pendant une **durée limitée** définie en fonction de l'objectif poursuivi par la collecte des données personnelles.

Les objectifs poursuivis par cette collecte sont multiples, notamment : gérer le DMST, mener des recherches, renseigner le dossier consacré à l'entreprise, gérer au plan des ressources humaines les salariés du SPST, administrer le SPST, etc.

› Pour plus d'informations sur la durée de conservation applicable au DMST, voir la fiche n° 10 du guide.

Pendant cette durée, trois phases successives doivent être distinguées :

1. Les données personnelles sont nécessaires pour la gestion courante du SPST : la conservation en « base active »

Lorsque les informations sont nécessaires au bon fonctionnement du SPST, elles sont **accessibles dans leur environnement de travail par les membres habilités du personnel** du SPST. On dit alors que les données personnelles sont conservées en « base active ».

Cette étape concerne **l'utilisation des données personnelles relatives aux travailleurs**, dans le cadre des recherches, enquêtes et études menées par les SPST notamment pour évaluer les risques professionnels au sein d'une entreprise déterminée, pour rédiger la fiche d'entreprise, etc.

Cette étape concerne également les **données relatives aux professionnels exerçant au sein des SPST** ou, plus largement, **les coordonnées des personnes** utilisées pour administrer et assurer le fonctionnement du SPST (p. ex. : organisation des relations entre les adhérents et le SPST interentreprises, organisation des instances, gestion des ressources humaines, etc.).

2. Les informations ne sont plus nécessaires à la gestion courante mais présentent un intérêt spécifique : la conservation en archivage intermédiaire (ou « base intermédiaire »)

Lorsque **l'objectif de la collecte de ces données est considéré comme atteint**, il n'est plus utile de disposer des données personnelles recueillies. Par conséquent, quand il est responsable de traitement, le SPST **n'a a priori plus besoin de conserver les données** dans son environnement de travail immédiat, autrement dit en « base active ».

Toutefois, ces données peuvent encore présenter un intérêt notamment administratif pour répondre à **une éventuelle obligation légale**. Elles peuvent alors être conservées en archivage intermédiaire, où elles pourront être consultées, de manière ponctuelle et motivée, par des personnes spécifiquement habilitées.

Exemple
En ce qui concerne les bulletins de paie des professionnels exerçant au sein du SPST interentreprises, une fois qu'ils sont émis et remis aux professionnels, ils n'ont plus besoin d'être conservés en « base active ». Ils doivent alors faire l'objet d'un archivage intermédiaire pour répondre à l'obligation légale de conservation de cinq ans, posée par le code du travail.

Une fois la durée de conservation en archivage intermédiaire expirée, les informations doivent être supprimées ou anonymisées.

Attention

L'archivage intermédiaire n'est ni systématique ni automatique : sa nécessité doit être évaluée au cas par cas par le SPST, sur la base d'une analyse détaillée. Un tri doit être effectué afin de n'archiver que les données nécessaires pour satisfaire l'objectif poursuivi par l'archivage intermédiaire.

3. Les informations présentent un intérêt public : la conservation en archivage définitif

L'archivage définitif déroge au principe de durée de conservation limitée et **permet d'archiver des informations sans limitation de durée**, dans des **conditions très strictes**.

Cette phase concerne uniquement les fichiers mis en œuvre à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

En pratique

Pour les fichiers et bases de données (hors dossier médical en santé au travail), les professionnels du SPST doivent définir une durée de conservation des données qui soit **proportionnée et cohérente avec l'objectif de la collecte des données personnelles**, c'est-à-dire le but poursuivi (voir fiche 1 du guide).

Le schéma de synthèse ci-dessous recense les différentes durées de conservation susceptibles d'être retenues par les professionnels du SPST, en tenant compte des objectifs poursuivis par les principaux fichiers ou bases de données utilisés au sein des SPST :

Attention

Ces durées de conservation ne constituent qu'un point de repère, une proposition. Les professionnels du SPST sont libres de s'en éloigner. Le choix retenu pour la durée de conservation doit être justifié et documenté.

Quelle durée de conservation retenir pour les fichiers déployés au sein des SDST (hors DMST) ?

RENSEIGNER LE DOSSIER CONSACRÉ À L'ENTREPRISE EMPLOYEUR	MENER DES RECHERCHES, ÉTUDES ET ENQUÊTES	GERER LES PROFESSIONNELS DU SPST AU PLAN DES RESSOURCES HUMAINES	ADMINISTRER LE SPST
Il s'agit du fichier constitué notamment pour rédiger la fiche d'entreprise et mener toutes les actions en lien avec les missions imparties aux SPST (conduite des actions en santé au travail, actions menées pour diminuer les risques professionnels, etc.).	Il s'agit des fichiers constitués dans le cadre des enquêtes menées par le SPST pour fournir des indicateurs en santé au travail, identifier des affections pouvant être provoquées ou aggravées par une activité professionnelle, cibler les actions de santé au travail à mettre en œuvre pour préserver la santé physique et mentale des travailleurs, etc.	Il s'agit des fichiers constitués pour gérer les personnels salariés exerçant leurs missions au sein des SPST.	Il s'agit des fichiers constitués pour la gestion du fonctionnement du SPST : tenue des instances, relations avec les contacts des adhérents, les contacts fournisseurs, etc.
Base active Pour les SPST autonomes et interentreprises : à déterminer au niveau du SPST **Archivage intermédiaire** Pour les SPST autonomes et interentreprises : à déterminer par le SPST	**Base active** (voir fiche n° 12) **Archivage intermédiaire** (voir fiche n° 12)	**Base active** Pour plus d'informations, voir le référentiel « Gestion des ressources humaines » **Archivage intermédiaire** Pour plus d'informations, voir le référentiel « Gestion des ressources humaines »	**Base active** À déterminer par le responsable de traitement en fonction de la finalité et des catégories des différents fichiers constitués **Archivage intermédiaire** À déterminer par le responsable de traitement en fonction de la finalité et des catégories des différents fichiers constitués

Les questions à se poser

- Un texte définit-il la durée de conservation des données ?
- La durée de conservation envisagée est-elle **adaptée au regard de l'objet de la collecte** des données personnelles ?
- La **réflexion menée pour justifier** la durée de conservation définie est-elle bien **justifiée et documentée** ?
- Des **mesures techniques ou organisationnelles** ont-elles été définies pour **supprimer régulièrement** les données personnelles à l'expiration des durées de conservation retenues ?
- Si un **délégué à la protection des données** a été désigné, celui-ci a-t-il été sollicité pour échanger sur la durée de conservation des informations ?
- La durée de conservation est-elle inscrite au sein du **registre des activités de traitement** ? (voir fiche n° 9) ;
- La durée de conservation a-t-elle été précisée dans les **mentions d'information communiquées aux personnes concernées** (ex : salariés du SPST, personnes contacts des entreprises adhérentes à un SPST, etc.) ? (voir fiche n° 6) ;
- La **séparation entre la « base active » et la « base d'archivage intermédiaire »** a-t-elle été opérée (par voie technique ou via le dispositif de gestion des habilitations et des accès) ?
- Des **mesures de sécurité** ont-elles été prévues pour protéger les informations (destruction, perte, altération, diffusion ou accès non autorisés) ?
- La **destruction des informations ou leur anonymisation** est-elle réalisée une fois que la durée de conservation ou la durée d'archivage intermédiaire fixée est atteinte ?

POUR ALLER PLUS LOIN

- Article 5.1.e du RGPD (durées de conservation des données), cnil.fr
- Article 89 du RGPD (garanties et dérogations pour la recherche ou les fins archivistiques), cnil.fr
- Article R. 4624-45-9 du code du travail (informations sur la santé des travailleurs), legifrance.gouv.fr
- Avis 05/2014 du 10 avril 2014 du CEPD sur les techniques d'anonymisation, ec.europa.eu
- Référentiel relatif à la gestion du personnel ; mis en œuvre aux fins de gestion du personnel (novembre 2019), cnil.fr
- Guide pratique « durée de conservation » - juillet 2020 (PDF, 763 ko), cnil.fr

FICHE N° 6 : COMMENT LE SPST INFORME-T-IL LES PERSONNES CONCERNÉES DE L'UTILISATION DE LEURS DONNÉES PERSONNELLES ?

Règles de droit

Les professionnels du service de prévention et de santé au travail (SPST) doivent fournir une information à la fois complète, concise, transparente, compréhensible et aisément accessible aux personnes concernées (travailleurs suivis par le SPST, salariés et adhérents des SPST interentreprises, etc.), afin que ces dernières comprennent l'objectif poursuivi et les modalités pratiques de l'utilisation de leurs données personnelles.

Cette obligation de transparence doit permettre à la personne concernée de garder la maîtrise de ses données personnelles et de faciliter l'exercice de ses droits.

Les personnes concernées par une collecte et une utilisation de leurs données personnelles doivent être informées, qu'il s'agisse :

- d'une **collecte directe** des informations.

> **Exemple**
>
> Lorsque les professionnels de santé du SPST recueillent directement auprès du travailleur des informations (ex : données de santé collectées lors d'une consultation de suivi du travailleur) ou encore lorsque les personnes en charge de la gestion du personnel du SPST interentreprises recrutent un intervenant en prévention des risques professionnels (p. ex. : collecte du CV, de la lettre de motivation et des informations données à l'occasion de l'entretien d'embauche) ;

- ou d'une **collecte indirecte** d'informations : lorsque les informations ne sont pas recueillies directement auprès des personnes concernées.

> **Exemple**
>
> Des informations peuvent être récupérées auprès de l'employeur du travailleur lorsque l'employeur, ayant connaissance de la date de la fin de l'arrêt de travail, saisit le SPST pour qu'il organise la visite de reprise après un congé maternité, une absence pour cause de maladie professionnelle ou une absence d'au moins trente jours pour cause d'accident du travail ou une absence d'au moins soixante jours pour cause de maladie ou d'accident non professionnels. En cas de collecte indirecte, les professionnels du SPST informent les personnes concernées **dès que possible et, au plus tard, dans un délai d'un mois**.

Les personnes concernées doivent également être informées dans le cas où :

- les modalités pratiques d'utilisation des données personnelles sont modifiées de manière substantielle (p. ex. : nouvel objectif, nouveau destinataire) ;
- un événement particulier a eu lieu (p. ex. : divulgation des données personnelles).

En pratique

Les professionnels du SPST doivent fournir diverses informations aux personnes concernées, dont les données personnelles sont traitées.

Dans tous les cas	Selon les caractéristiques du fichier
L'**identité et les coordonnées de l'organisme, responsable de traitement**.	En cas de collecte auprès d'un autre organisme et non auprès de la personne : les **catégories d'informations** recueillies et la source de la collecte.
Les **coordonnées du délégué à la protection des données**.	Des précisions sur **les intérêts légitimes** poursuivis par le responsable de traitement s'il y en a.
L'**objectif poursuivi par l'utilisation des informations**, c'est-à-dire à quoi elles vont servir.	Les **catégories d'informations recueillies et la source de la collecte.**
La **base légale** du fichier c'est-à-dire ce qui justifie que le responsable de traitement est autorisé à créer un fichier contenant des données personnelles : - existe-t-il un intérêt légitime pour recueillir les données personnelles dont les professionnels du SPST ont besoin pour l'exercice de leurs missions ? - existe-t-il une obligation légale spécifique prévue par un texte, notamment le code du travail ?	Le cas échéant, l'existence d'un **transfert** d'informations vers un pays hors de l'Union européenne ainsi que les **garanties associées**.
Les **destinataires ou catégories de destinataires des informations** (qui a besoin d'y accéder ou de les recevoir au vu de l'objectif de la collecte des données personnelles).	

En plus, le responsable du traitement doit fournir les informations suivantes nécessaires pour garantir un traitement équitable et transparent

- Les **durées de conservation des données** (ou les critères permettant de la déterminer) ;
- les **droits des personnes concernées** (voir la fiche n° 7), doivent au moins être mentionnés les droits d'accès, de rectification, d'effacement et à la limitation qui sont applicables pour tous les fichiers) ;
- le **droit d'introduire une réclamation auprès de la CNIL** :

- besoin pour l'exercice de leurs missions ?
- existe-t-il une **obligation légale spécifique** prévue par un texte, notamment le code du travail ?

- le **caractère obligatoire ou facultatif du recueil des informations** et les éventuelles conséquences pour les personnes en cas de non-fourniture des données. L'information fournie aux personnes concernées doit par ailleurs remplir trois conditions. Elle doit ainsi être :
- **complète** : les professionnels du SPST doivent donner un **panorama complet** des caractéristiques concrètes de l'utilisation des données personnelles en fournissant un certain nombre d'éléments obligatoires ;
- **compréhensible** : les éléments d'informations doivent être les plus clairs et les plus précis possibles. Pour cela, il faut veiller à :
  - utiliser un **vocabulaire simple** ;
  - **réaliser une mention d'information aussi courte et lisible que possible**.
- **accessible** : les personnes concernées ne doivent pas rencontrer de difficultés en recherchant l'information.

Exemple

Les membres de l'équipe pluridisciplinaire du SPST peuvent fournir un document précisant l'ensemble des informations relatives à la gestion du DMST en même temps que la convocation à la première visite ou que la remise de la fiche de renseignement. Cette fiche est à compléter préalablement au rendez-vous avec le médecin du travail lors de la première visite, puis lors des visites suivantes si les modalités d'utilisation ont fait l'objet de modifications substantielles. Un modèle de notice d'information concernant le traitement de données personnelles utilisé pour gérer le DMST figure en annexe n° 4.

Attention

Cette obligation de transparence doit se traduire par une adaptation des modalités d'information à la personne concernée.
Cela signifie par exemple que si le SPST est amené à prendre en charge des travailleurs atteints d'une altération cognitive, il est procédé à une information dans un langage compréhensible et selon des modalités appropriées à leur situation.

Afin d'être concise et accessible, l'information peut s'effectuer en deux étapes, c'est-à-dire en priorisant les informations essentielles (identité du responsable de traitement, objectif poursuivi par cette utilisation et droits des personnes), tout en en offrant un accès simple aux autres caractéristiques pratiques comme un renvoi à un document consultable en ligne ou la possibilité de disposer d'une information complète mise à disposition dans les services du SPST.

À noter

Quelle que soit la catégorie de personnes concernées (travailleurs, salariés du SPST, contacts des SPST interentreprises au sein des entreprises adhérentes, prestataires externes, etc.), les professionnels du SPST doivent faire preuve de transparence et fournir une notice d'information dès lors que des données personnelles font l'objet d'une utilisation.
Par exemple, les salariés du SPST interentreprises doivent connaître les caractéristiques pratiques de l'utilisation de leurs données personnelles dans le cadre de la gestion des ressources humaines : gestion de la paie, gestion de l'action sociale ou encore restauration collective.

Les questions à se poser

- Les caractéristiques pratiques d'utilisation des données personnelles devant obligatoirement être portées à la connaissance de la personne concernées ont-elles été fournies ?
- L'information est-elle **facilement présentée et adaptée** aux personnes concernées ?

POUR ALLER PLUS LOIN

- Article 12 du RGPD (transparence et modalité d'exercice des droits des personnes), cnil.fr
- Article 13 du RGPD (informations à fournir en cas de collecte auprès de la personne concernée), cnil.fr
- Article 14 du RGPD (informations à fournir en cas de collecte indirecte de données), cnil.fr
- Lignes directrices du CEPD sur la transparence, adoptées le 29 novembre 2017 - version révisée et adoptée le 11 avril 2018 (PDF, 509 ko), cnil.fr

FICHE N° 7 : QUELLES MESURES LE SPST DOIT-IL PRENDRE POUR GARANTIR LES DROITS DES PERSONNES CONCERNÉES ?

Règles de droit

Les travailleurs ainsi que les autres personnes concernées (personnels des services de prévention et de santé au travail (SPST), adhérents des SPST interentreprises, etc.) disposent de droits afin de garder la maîtrise de leurs données personnelles. Le SPST doit leur expliquer comment les exercer dans le cadre de son obligation de transparence via une information intervenant au plus tard au moment de la première visite. Cette information peut prendre la forme de la remise d'une fiche d'information.

› Pour plus d'informations sur l'obligation de transparence, voir la fiche n°6 du guide.

Par ailleurs, lorsqu'elles exercent leurs droits, les personnes concernées doivent obtenir une réponse avant un mois.

Dans le cadre des fichiers mis en œuvre par les SPST, les personnes concernées disposent d'un socle de droits. Elles peuvent ainsi :

- **accéder** à leurs données personnelles ;
- demander qu'elles soient **rectifiées** ;
- les faire **effacer** ;
- les « **geler** », c'est-à-dire les maintenir en l'état (droit à la limitation).

Ces droits permettent aux personnes concernées de prendre une part active dans la gestion des données personnelles les concernant :

DROIT D'ACCÈS

- Une personne concernée peut demander aux professionnels du SPST la confirmation que ce dernier détient des informations sur elle et la communication de ces dernières pour en vérifier le contenu.
- Dans le cadre d'une telle demande, les personnes compétentes au sein du SPST peuvent être amenées à rappeler les caractéristiques de l'utilisation des informations (par exemple : objectifs, catégories d'informations traitées, destinataires, durée de conservation).
- Attention, certaines dispositions particulières du code du travail s'appliquent, notamment celles relatives à l'accès au dossier médical en santé au travail.

DROIT DE RECTIFICATION

Une personne concernée peut demander que ses informations soient rectifiées si elles sont inexactes ou incomplètes. Ce droit permet d'éviter que le SPST utilise ou diffuse des informations erronées.

DROIT À L'EFFACEMENT

Une personne concernée est notamment en droit d'exiger l'effacement de ses données personnelles si :

- les informations ne sont plus nécessaires au SPST au regard de l'objectif poursuivi par la collecte et l'utilisation des données ;
- les informations ont fait l'objet d'un traitement illicite (p. ex.: collecte de données qui n'avaient pas à être traitées – sur ce point, voir la fiche n° 10 sur le DMST) ;
- les informations doivent être effacées pour respecter une obligation légale.

Attention
Selon l'article 17.3.b) et c) du RGPD, le droit à l'effacement peut être écarté lorsque le traitement est nécessaire « *pour des motifs d'intérêt public dans le domaine de la santé publique* » et, en particulier, pour les fichiers qui sont constitués « *aux fins de la médecine préventive, de la médecine du travail, de l'appréciation de la capacité de travail du travailleur , de diagnostics médicaux, de la prise en charge sanitaire ou sociale ou de la gestion des systèmes et des services de soins de santé ou de protection sociale* » *mais également pour les traitements constitués pour « respecter une obligation légale »* (cas du DMST). Par conséquent, le SPST peut ne pas répondre favorablement à la demande d'un travailleur d'effacer des données de son DMST.

DROIT À LA LIMITATION OU « GEL » DES DONNÉES

Une personne concernée peut demander à « geler » l'utilisation de ses données personnelles dans deux situations :

- si elle conteste l'exactitude des données, le temps que les professionnels du SPST effectuent une vérification ;
- si l'organisme souhaite supprimer les données mais que la personne concernée souhaite quant à elle les conserver, notamment pour exercer un autre droit, en cas de contentieux par exemple.

Parallèlement à ce socle de droits, les personnes concernées peuvent disposer de droits complémentaires conditionnés au fondement légal du fichier, c'est-à-dire à la justification permettant de le mettre en œuvre.

DROIT D'OPPOSITION

Si le fichier n'est pas fondé sur une obligation légale mais sur l'intérêt légitime du SPST (cas des fichiers utilisés pour la gestion des salariés, des adhérents, etc.), la personne concernée a le droit de s'opposer à l'utilisation de ses informations. Le responsable de traitement doit alors cesser d'utiliser ces informations sauf s'il est en mesure de justifier de l'existence de motifs légitimes et impérieux prévalant sur les intérêts et les droits et libertés de la personne concernée.

En pratique, les personnes concernées peuvent exercer les droits suivants :

Fondements légaux habituellement utilisés au sein des SPST pour justifier la création de fichiers et de bases de données	Exemples de finalités	Accès	Rectification	Effacement	Limitation	Opposition
Obligation légale	Gestion du dossier médical en santé au travail Élaboration de la fiche d'entreprise	✓	✓	Exercice possible de ce droit, selon les cas	✓	✗
Intérêt légitime	Réalisation de recherches, études et enquêtes Gestion des salariés du SPST Administration du SPST Fichier des adhérents	✓	✓	✓	✓	✓

Attention
Le tableau ci-dessus reprend les fondements légaux habituellement utilisés au sein des SPST. Le recours à la base légale de la mission d'intérêt public peut également fonder les traitements mis en œuvre par les autorités publiques aux fins d'exécuter leurs missions.

En pratique

Lorsqu'il reçoit une demande d'exercice d'un droit, le responsable de traitement (généralement le SPST) doit procéder en cinq étapes :

1. Vérifier que le droit visé par la demande est compatible avec le fondement légal du fichier
2. Analyser la demande sans la subordonner à certains préalables tels que justifications, paiement, signature de document, etc.
3. S'assurer de l'identité du demandeur qui peut être le travailleur, un salarié du SPST interentreprises, etc.
4. Répondre dans les meilleurs délais sans dépasser 1 mois
5. Communiquer des informations compréhensibles en explicitant les codes, sigles et abréviations

Afin de pouvoir être en mesure de répondre aux demandes d'exercice des droits des personnes concernées dans les délais prévus par les textes, il est recommandé de définir une procédure en collaboration avec le délégué à la protection des données afin de :

- définir les rôles de chacun pour être en mesure de répondre aux personnes concernées, notamment les travailleurs ;
- encadrer temporellement les différentes étapes de gestion de la demande.

À noter

Si, par principe, aucun paiement ne peut être exigé, des frais raisonnables liés à une demande particulière (p. ex. : demande d'une copie supplémentaire) pourront être demandés dans des situations exceptionnelles.

De plus, si la demande d'exercice d'un droit est complexe à traiter ou si le SPST doit faire face à de nombreuses demandes, il peut fournir au demandeur une réponse dans un délai de **trois mois (au lieu d'un)**, sous réserve qu'il l'en ait informé et qu'il lui ait indiqué les motifs justifiant le report de sa réponse.

Attention

S'agissant de la vérification de la qualité du demandeur, le professionnel du SPST en charge de l'exercice des droits ne doit pas automatiquement demander une pièce d'identité à la personne concernée souhaitant exercer un droit (par exemple, lorsqu'un **travailleur utilise sa messagerie électronique professionnelle sécurisée** pour effectuer une demande d'exercice des droits, il n'apparaît pas nécessaire de demander un justificatif d'identité).

Les questions à se poser

- Quelle est la justification expliquant l'utilisation des données personnelles (existe-t-il une obligation légale prévue par un texte ? à défaut, existe-t-il un intérêt légitime à le créer ?) permettant de **déterminer les droits susceptibles de pouvoir être exercés** par les personnes concernées ?
- Les personnes concernées ont-elles été **informées de la possibilité d'exercer leurs droits** et des modalités pour le faire ? (voir la fiche n°6 sur l'information des personnes concernées)
- **Les rôles et les étapes en interne** ont-ils été encadrés pour être en mesure de répondre aux demandes d'exercice des droits dans un délai d'un mois ?
- En cas de demande d'accès ou de copie des informations, **les éléments susceptibles de ne pas être compris par la personne** concernée (sigles, abréviations, etc.) ont-ils été **explicités** ?

POUR ALLER PLUS LOIN

- Article 15 du RGPD (droit d'accès), cnil.fr
- Article 16 du RGPD (droit de rectification), cnil.fr
- Article 17 du RGPD (droit à l'effacement), cnil.fr
- Article 18 du RGPD (droit à la limitation), cnil.fr
- Article 21 du RGPD (droit d'opposition au profilage et à la prise de décision automatisée), cnil.fr

FICHE N° 8 : COMMENT LE SPST PEUT-IL GARANTIR LA SÉCURITÉ DES INFORMATIONS TRAITÉES ?

Règles de droit

Lorsqu'il est responsable de traitement d'un fichier ou d'une base de données, le service de prévention et de santé au travail (SPST) doit s'assurer de l'application des règles en matière de sécurité et de confidentialité. Il peut faire appel soit à des compétences internes soit à des experts externes de la sécurité des systèmes d'information.

Toutes les précautions utiles adaptées aux risques pour préserver la sécurité et la confidentialité des données personnelles recueillies sur les personnes concernées (travailleurs, personnels des SPST, adhérents des SPST interentreprises, etc.) doivent être prises. Il faut **empêcher que des données personnelles soient sujettes à un accès illégitime, une modification non désirée, ou une disparition**.

Un grand nombre d'informations utilisées par les SPST concernent l'état de santé des travailleurs et figurent dans leur dossier médical en santé au travail (DMST). Les informations présentes dans le DMST sont considérées comme sensibles par le RGPD. Leur collecte, leur utilisation, leur conservation obéissent à un régime particulier (voir la fiche n° 10). Ces données étant protégées par le secret professionnel, en particulier le secret médical, leur traitement exige au plan technique :

- un niveau de sécurité adapté ;
- la mise en place d'une politique très rigoureuse de gestion des habilitations et des accès (qui accède à quelles informations au regard des missions qu'il exerce) pour éviter que des personnes non autorisées accèdent au DMST (p. ex.: les personnes en charge des ressources humaines dans une entreprise). La Haute Autorité de santé (HAS) recommande que le médecin du travail soit seul responsable de la gestion des habilitations et des accès au DMST.

En pratique

Les mesures de sécurité à mettre en place au niveau du SPST sont multiples. Elles doivent être déterminées par des compétences internes ou des experts externes de la sécurité des systèmes d'information, au regard d'une analyse de risques prenant en compte les spécificités de chacun des fichiers ou bases de données constituées (nature des informations, volume, risques pour les personnes concernées, etc.).

L'analyse d'impact relative à la protection des données (AIPD) est un outil qui permet au SPST, lorsqu'il est responsable de traitement, de concevoir un futur traitement conforme au RGPD, notamment sur le plan de la sécurité. La réalisation d'une AIPD favorise **l'évaluation des risques pesant sur la sécurité des données personnelles recueillies** (confidentialité, intégrité et disponibilité) ainsi que des impacts potentiels sur la vie privée des personnes concernées (travailleurs, personnels des SPST, etc.) si ces risques se concrétisaient.

› Pour plus d'informations sur l'AIPD, nous vous invitons à consulter la fiche n° 9.

Cette démarche contribue à déterminer les mesures techniques et organisationnelles à mettre en place au niveau du SPST pour limiter les risques. Le guide sur la sécurité des données personnelles publié par la CNIL sur son site Internet peut servir de base pour établir ces mesures de sécurité.

Parmi les mesures, un travail de **sensibilisation des personnels** exerçant au sein du SPST sur les règles applicables en matière de sécurité et de vie privée est fortement recommandé.

Une attention particulière doit être portée aux mesures suivantes :

ACTIONS	MESURES
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes manipulant les données
	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	Définir un identifiant (« *login* ») unique pour chaque utilisateur
	Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL
	Obliger l'utilisateur à changer le mot de passe attribué automatiquement ou par un administrateur
	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	Définir des profils d'habilitation
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
Tracer les opérations et gérer les incidents	Prévoir un système de journalisation
	Informer les utilisateurs de la mise en place du système de journalisation
	Protéger les équipements de journalisation et les informations journalisées
	Prévoir les procédures et les responsabilités internes pour la gestion des incidents, dont la procédure de notification aux régulateurs des violations de données personnelles
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session
	Utiliser des antivirus régulièrement mis à jour
	Installer un pare-feu (« firewall ») logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des smartphones
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Sécuriser ses réseaux Wi-Fi, notamment en mettant en œuvre le protocole WPA3
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées

ACTIONS	MESURES
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou donnée personnelle ne passe par les URL
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les *cookies* non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr
	Protéger les sauvegardes, notamment durant leur convoyage
	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer les développements informatiques	Prendre en compte la protection des données personnelles dès la conception
	Proposer des paramètres respectueux de la vie privée par défaut
	Éviter les zones de commentaires ou les encadrer strictement
	Utiliser des données fictives ou anonymisées pour le développement et les tests
Encadrer la maintenance et la fin de vie des matériels et des logiciels	Enregistrer les interventions de maintenance dans une main courante
	Encadrer les interventions de tiers par un responsable de l'organisme
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir des clauses spécifiques dans les contrats des sous-traitants
	Prévoir les conditions de restitution et de destruction des données
	S'assurer de l'effectivité des garanties prévues (ex. : audits de sécurité, visites)
Sécuriser les échanges avec d'autres organismes	Chiffrer les données avant leur envoi
	S'assurer qu'il s'agit du bon destinataire
	Transmettre le secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
	Installer des alarmes anti-intrusion et les vérifier périodiquement
Chiffrer, hacher ou signer	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues et sécurisées

Attention

Concernant le DMST, compte tenu de la sensibilité des données personnelles présentes dans celui-ci, des mesures de sécurité spécifiques s'appliquent (notamment la conformité à des référentiels de sécurité, la politique de gestion des habilitations et des accès, le cas échant le recours à un hébergeur de données de santé certifié (ou agréé selon la réglementation applicable)).

Pour plus d'informations sur les mesures de sécurité à respecter s'agissant du DMST, voir la fiche n° 10.

Par ailleurs, le médecin du travail joue un rôle particulier dans la politique de gestion des habilitations et des accès au DMST.

Pour plus d'informations sur ce rôle, voir la fiche n° 11.

En pratique, **la réalisation d'une AIPD est nécessaire pour le fichier utilisé pour la gestion des DMST, dans la mesure où celui-ci peut faire courir un risque important pour les travailleurs** (volume important des données personnelles de nature sensible les concernant). En revanche, elle ne sera pas obligatoire pour le fichier utilisé pour la gestion des prestataires et des organismes adhérents.

Les questions à se poser :

- Les mesures mises en place pour assurer la confidentialité, l'intégrité et la disponibilité des données personnelles sont-elles conformes à la réglementation sur la protection des données personnelles et **adaptées au type de fichier ou de base de données mis en œuvre** ?
- Les **professionnels ont-ils effectivement besoin, au regard de leurs missions, d'accéder aux informations recueillies par les SPST**, en particulier celles en lien avec l'état de santé des travailleurs ?
- Une **procédure de gestion des habilitations** et des accès est-elle mise en place entre les professionnels qui partagent des informations ?
- Concernant le traitement utilisé pour gérer le dossier médical en santé au travail, les règles de sécurité spécifiques sont-elles respectées ? (voir la fiche n° 10).

POUR ALLER PLUS LOIN

- Article 5.1.f du RGPD (intégrité et confidentialité), cnil.fr
- Article 32 du RGPD (sécurité du traitement), cnil.fr
- Article 35 du RGPD (analyse d'impact relative à la protection des données), cnil.fr
- Guide sur la sécurité des données personnelles – édition 2023 (PDF, 641 ko), cnil.fr

FICHE N° 9 : COMMENT LE SPST PEUT-IL ATTESTER DE SA CONFORMITÉ AU RGPD ?

Règles de droit

Lorsque le SPST est responsable de traitement (fichier, base de données), sa direction doit être en mesure de **démontrer, à tout moment, le respect des règles en matière de protection des données personnelles**. Cette documentation permet à la fois de :

- **suivre les actions réalisées au sein du SPST**. Il s'agit d'être en mesure de les réexaminer et de les actualiser, si cela s'avère nécessaire, afin d'assurer en continu la protection des données personnelles utilisées ;
- **justifier** auprès de la CNIL **des actions entreprises afin de démontrer la conformité**.

Dans certains cas, le SPST devra procéder à des formalités préalablement à la création d'un fichier ou d'une base de données :

LE SPST DOIT-IL EFFECTUER UNE FORMALITÉ ?

OUI

Recherches, études ou enquêtes multicentriques ou impliquant que les informations soient rendues accessibles en dehors de l'équipe du SPST.

Sur les recherches, études ou enquêtes menées par les SPST et la nature de la formalité à accomplir (déclaration de conformité à une méthodologie de référence ou demande d'autorisation), voir la fiche n° 12.

NON

Fichiers mis en œuvre pour la gestion du dossier médical en santé au travail

Fichiers utilisés à des fins de recherches « internes », réalisés à partir des informations recueillies dans le cadre du suivi du travailleur par le personnel du SPST assurant ce suivi et pour leur usage exclusif

Fichiers qui ne sont pas dans le domaine de la santé : organisation du travail, gestion de la rémunération ou de la base de données adhérents dans les SPST interentreprises, etc.

Pour les SPST amenés à traiter à grande échelle des informations de santé, la désignation d'un **délégué à la protection des données dans leur organisme** (DPO) est en principe obligatoire. Le DPO est en charge du pilotage des démarches de mise en conformité au RGPD.

> Pour plus d'informations sur les DPO, voir « Le délégué à la protection des données (DPO) » sur cnil.fr.

En pratique

Pour tous les fichiers et bases de données, qu'ils nécessitent ou non d'obtenir l'autorisation de la CNIL, les SPST doivent documenter leurs démarches de mise en conformité en menant principalement les trois actions suivantes :

Action n° 1 : veiller à l'inscription des fichiers et bases de données au registre des activités de traitement

Ce document permet à la fois de piloter la conformité au RGPD dans les structures et de démontrer la conformité du SPST aux règles relatives à la protection des données personnelles. Sous format papier ou électronique, ce document doit donc **être conservé au sein du SPST**.

Le registre des activités de traitement recense les différentes utilisations des fichiers ou bases de données qui sont créés par le SPST, et notamment :

- **les parties prenantes** à l'utilisation des données personnelles (responsable de traitement, co-responsables, sous-traitant) ainsi que **les rôles et responsabilités de chacune d'elles** ;
- **les catégories de données personnelles** traitées au sein du SPST (p. ex.: informations relatives à la santé des travailleurs, informations d'identification des personnels exerçant au sein des SPST, informations permettant d'identifier des adhérents pour les SPST interentreprises) ;
- **l'objectif poursuivi par le fichier** : gérer le dossier médical en santé au travail, mener une étude sur les risques professionnels au sein d'une entreprise déterminée, gérer la paie des salariés d'un SPST interentreprises, etc. ;
- **qui accède aux données personnelles et à qui elles sont communiquées** ;
- si des **transferts d'informations vers des pays situés hors de l'UE** sont prévus et, dans ce cas, les garanties associées à ces transferts ;
- **combien de temps les données sont conservées** ;
- **comment les données sont sécurisées**.

Attention

Lorsque le SPST est responsable de traitement, il conviendra de veiller à justifier les choix réalisés c'est-à-dire de **démontrer en quoi les modalités pratiques de l'utilisation des données personnelles sont appropriées à chacune des situations concernées**.

Par exemple, plusieurs textes du code du travail peuvent fournir des indications sur la durée de conservation, notamment en ce qui concerne le DMST pour lequel il est prévu des durées propres de conservation en particulier pour les travailleurs exposés à des risques particuliers dans leur exercice professionnel, tels des agents pathogènes ou cancérogènes. Pour la gestion du traitement utilisé à des fins de gestion du personnel, les dispositions du code du travail applicables à la durée de conservation des bulletins de paie doivent être respectées.

Afin d'avoir une documentation complète, **divers documents doivent être annexés au registre** : audit de sécurité, contrat de sous-traitance, etc.

La fiche de registre d'un fichier est un **document évolutif**. Cela signifie qu'elle doit être mise à jour à chaque évolution apportée à l'utilisation des données (mesures de sécurité, nouveau destinataire, nouvelles données collectées, modification de la durée de conservation, etc.) afin de fournir une vue d'ensemble actualisée.

Des modèles de fiches de registre des activités de traitement sont présentés en annexe n° 3 du guide.

Action n° 2 : réaliser une analyse d'impact relative à la protection des données (AIPD) pour les fichiers présentant un risque élevé pour les personnes concernées

Une AIPD aide les organismes à utiliser les données personnelles de façon à respecter la vie privée, lorsque cette utilisation est susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées.

Une AIPD doit être menée par le SPST, 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.) ;
- d'informations relatives à des **personnes** considérées comme **vulnérables**, dans la mesure où l'utilisation des données intervient dans un environnement de travail.

Une AIPD se décompose en trois parties :

> **Exemple**
>
> Pour l'utilisation de données personnelles à des fins de gestion des **DMST**, la réalisation d'une AIPD apparaît nécessaire dans la mesure où cette utilisation de données personnelles suppose un volume important de données personnelles de nature sensible. En revanche, une AIPD n'apparaît pas nécessaire lorsque des données personnelles sont utilisées dans le cadre de la gestion des prestataires ou de l'organisation des relations avec les organismes adhérant à un SPST interentreprises.

- une **description détaillée** de l'utilisation qui est faite des données personnelles, comprenant tant les **aspects techniques qu'opérationnels** ;
- **l'évaluation,** de nature plus juridique, de la **nécessité et de la proportionnalité** concernant les principes et droits fondamentaux (objectifs poursuivis, nature des données personnelles et durées de conservation, information et droits des personnes, etc.) devant impérativement être respectés, quels que soient les risques ;
- **l'étude**, de nature plus technique, **des risques sur la sécurité des informations** (confidentialité, intégrité et disponibilité) ainsi que leur impact potentiel sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données personnelles.

Attention

L'AIPD devant permettre de limiter au minimum les risques pour les droits et libertés des personnes concernées (travailleurs, salariés du SPST, contacts des adhérents du SPST, etc.), il est nécessaire de **mettre à jour l'AIPD à chaque fois que des modifications** sont apportées aux modalités d'utilisation des données personnelles, mais également afin de s'assurer de la prise en compte de l'évolution des connaissances techniques à même de garantir la sécurité et la confidentialité des informations. .

Action n° 3 : se tourner vers le délégué à la protection des données (DPO) en cas de doute

Le DPO **conseille et accompagne** l'organisme qui le désigne dans sa conformité.

Si le **SPST est autonome**, il peut, en cas de difficulté, se rapprocher du DPO de son organisme qui est dans l'obligation d'en désigner un*.

Si le **SPST est interentreprises**, il se trouve dans l'obligation de désigner un DPO dans la mesure où son activité de base consiste en l'utilisation à grande échelle de données sensibles.

› Pour plus d'informations sur le DPO, voir « Le délégué à la protection des données » sur cnil.fr.

Les questions à se poser

- **Une formalité** auprès de la **CNIL** est-elle obligatoire ?
- L'utilisation des données personnelles a-t-elle été inscrite dans le **registre des activités de traitement** ?
- **Les choix réalisés** (durées de conservation, informations collectées, etc.) ont-ils été justifiés dans le registre ?
- L'ensemble de la documentation relative aux modalités d'utilisation des données personnelles, notamment les contrats de sous-traitance indiquant précisément les répartitions des responsabilités et missions de chacune des parties a-t-il été intégré dans le registre ?
- Une AIPD doit-elle être réalisée ?
- **Le DPO a-t-il été contacté** préalablement à la mise en œuvre du fichier ?

POUR ALLER PLUS LOIN

- Articles 35 du RGPD (analyse d'impact relative à la protection des données), cnil.fr
- Article 37 du RGPD (désignation du délégué à la protection des données), cnil.fr
- Article 38 du RGPD (fonction du délégué à la protection des données), cnil.fr
- Article 39 du RGPD (missions du délégué à la protection des données), cnil.fr
- Article 57 de la loi Informatique et Libertés (obligations du responsable de traitement et du sous-traitant), cnil.fr
- Article 65 de la loi Informatique et Libertés (traitements concernant la santé des personnes)

*Les entreprises dotées d'un SPST autonome disposent d'une masse salariale supérieure à 500 salariés et sont ainsi amenées à mettre en œuvre des fichiers exigeant un suivi régulier et systématique à grande échelle des personnes concernées. Les autorités et organismes publics sont également dans l'obligation de désigner un DPO.

SPÉCIFICITÉS DES FICHIERS CONSTITUÉS PAR LES SPST POUR EXERCER LEURS MISSIONS : LE DOSSIER MÉDICAL EN SANTÉ AU TRAVAIL ET LES ÉTUDES ET ENQUÊTES

FICHE N° 10 : QUELLES SONT LES RÈGLES APPLICABLES AU DOSSIER MÉDICAL EN SANTÉ AU TRAVAIL ?

Règles de droit

Tout travailleur bénéficie, au titre de la surveillance de l'état de santé des travailleurs, d'un suivi individuel de son état de santé assuré par le médecin du travail, le médecin praticien correspondant et, sous l'autorité du médecin du travail, par le collaborateur médecin, l'interne en médecine du travail et l'infirmier. Pour assurer ce suivi, un dossier médical en santé au travail (DMST) est obligatoirement créé par ces professionnels de santé.

La loi n° 2021-1018 du 2 août 2021 pour renforcer la prévention en santé au travail et le décret n° 2022-1434 du 15 novembre 2022 relatif au dossier médical en santé au travail ont donné un nouveau cadre juridique au DMST, codifié aux articles R. 4624-45-3 et s. du code du travail.

Le SPST, représenté par sa direction, est le responsable de traitement du fichier utilisé aux fins de gérer le DMST. Il est juridiquement responsable de la bonne application des règles du code du travail et de celles applicables en matière de protection des données personnelles, en particulier en ce qui concerne l'étendue des données recueillies sur les travailleurs, leur durée de conservation, le contrôle de la gestion des accès par les personnels du SPST, la définition de mesures de sécurité à mettre en œuvre, etc.

› Pour plus d'informations sur la responsabilité de traitement, voir la fiche n° 2.
Pour apprécier la conformité du DMST au RGPD, nous vous invitons à consulter l'annexe n° 3.

Attention

Si le SPST est le responsable de traitement pour la gestion du DMST, seuls les professionnels de santé en charge du suivi individuel du travailleur (médecins du travail, collaborateurs médecins, médecins praticiens correspondants, internes en médecine du travail, infirmiers) et les autres membres de l'équipe pluridisciplinaire (p. ex.: ergonomes, toxicologues, assistants ou gestionnaires de service de santé au travail), placés sous la supervision du médecin du travail peuvent, consulter et alimenter toute ou partie du DMST. Ils sont responsables du contenu du DMST. En conséquence, les personnels non professionnels de santé ou n'appartenant pas à l'équipe pluridisciplinaire (personnel de direction et personnel administratif notamment) ne sont pas autorisés à en prendre connaissance, ni même à l'alimenter.

En pratique

CONTENU DU DMST

Le DMST est un fichier numérique contenant des données personnelles ayant pour finalité de permettre la traçabilité des expositions et de prévenir toute altération de la santé du travailleur du fait de son activité professionnelle et d'assurer son suivi médical.

Seules des informations **adéquates, pertinentes et limitées** à cet objectif (ce que l'on appelle le principe de minimisation), recueillies notamment à l'occasion des visites d'information et de prévention, de suivi individuel renforcé ou de pré-reprise, peuvent être enregistrées et conservées dans le DMST.

› Pour plus d'informations sur la responsabilité de traitement, voir la fiche n° 3.

Dans ce cadre et conformément au décret n° 2022-1434, il apparaît légitime que les professionnels de santé du SPST en charge du suivi individuel du travailleur et, sous l'autorité du médecin du travail, les autres membres de l'équipe pluridisciplinaire du SPST collectent et enregistrent certaines catégories d'informations relatives aux travailleurs, notamment :

- les **données d'identité et les données médico-administratives** du travailleur nécessaires à la coordination de sa prise en charge en matière de santé, ainsi que, le cas échéant, les données d'identité et de contact de son médecin traitant ;
- les informations permettant de connaître les **risques actuels ou passés auxquels le travailleur est ou a été exposé**, notamment les caractéristiques du ou des postes occupés ainsi que du secteur, les données d'exposition, les mesures de prévention mises en place ;
- les informations relatives à l'état de **santé du travailleur recueillies lors des visites et examens** ;
- les **correspondances échangées entre professionnels de santé** aux fins de la coordination et de la continuité de la prise en charge du travailleur ;
- les informations formalisées concernant les **attestations, avis et propositions des professionnels de santé au travail** ;
- la mention de **l'information du travailleur sur ses droits en matière d'accès aux données** le concernant et sur les conditions d'accès à son DMST ;
- pour l'organisation de son suivi individuel par le SPST, le **consentement ou l'opposition du travailleur** :

- à l'utilisation des technologies de l'information ou de la communication (ex : organisation de téléconsultations) ;
- à l'accès à son DMST (ex : cas particulier de la transmission du DMST d'un SPST à un autre SPST, si le travailleur relève de plusieurs services).

Attention

Pour chaque travailleur, l'identifiant du DMST est l'identifiant national de santé (INS) composé du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR), des noms, prénoms, sexe, date et lieu de naissance.

Le NIR peut donc être collecté par les professionnels du SPST. L'utilisation de l'INS est strictement encadrée par les articles L. 1111-8-1, R. 1111-8-1 et suivants du code de la santé publique ainsi que le référentiel consacré à l'INS (arrêté du 27 mai 2021).

Le tableau suivant recense des exemples de données, par catégorie, qui sont susceptibles d'être recueillies et utilisées, plus particulièrement par les membres de l'équipe pluridisciplinaire de santé au travail du SPST, (les exemples ne constituent pas une liste exhaustive des données pouvant être traitées) :

Catégories de données	Exemples de données personnelles pouvant être collectées
Informations d'identité et données administratives du travailleur, nécessaires à la coordination de sa prise en charge, le cas échéant, les données d'identité et de contact de son médecin traitant	• Nom, prénom, date et lieu de naissance pour identifier le travailleur • Employeur • Historique des rendez-vous avec le SPST • Identifiant national de santé (INS)
Informations permettant de connaître les risques actuels ou passés auxquels le travailleur est ou a été exposé	• Profession actuelle • Situation personnelle ou familiale • Horaires de travail et modalités des trajets entre son domicile et son lieu d'activité professionnelle • Description des activités ou tâches effectuées permettant d'identifier les risques • Risques identifiés et données d'exposition : nature des nuisances (physiques, chimiques, biologiques, organisationnelles, autres) • Mesures de prévention mises en place • Secteurs d'activité et professions antérieurs
Informations relatives à l'état de santé du travailleur recueillies lors des visites et examens	• Qualification de travailleur handicapé ou notion d'invalidité • Grossesse • Risques psycho-sociaux • Antécédents médicaux personnels, notamment ceux en lien avec un accident de travail, une maladie professionnelle ou une maladie à caractère professionnel (taux d'IP) • Élément de santé de nature à caractériser l'état de santé du travailleur lorsqu'il nécessite un aménagement de poste
Correspondances échangées entre professionnels de santé	• Toutes les correspondances rédigées aux fins de coordonner et d'assurer la continuité de la prise en charge
Informations formalisées concernant les attestations, avis et propositions des professionnels de santé au travail	• Proposition d'amélioration ou d'adaptation du poste de travail, de reclassement, etc. • Échanges avec l'employeur et le travailleur concernant les mesures individuelles d'aménagement, d'adaptation ou de transformation du poste de travail ou des mesures d'aménagement du temps de travail
Modalités d'exercice des droits des travailleurs	• Information du travailleur sur ses droits, en matière d'accès à son DMST • Le cas échéant, consentement ou opposition du travailleur concernant le recours à des pratiques de soins à distance, à la transmission de son DMST à un autre SPST

Attention

Même si les médecins du travail et, sous leur autorité, les autres professionnels alimentant le DMST, disposent d'une indépendance professionnelle/technique pour apprécier ce qui est utile ou non à la retranscription d'informations dans le DMST pour préserver la santé du travailleur, une attention particulière devra être portée au respect du principe de minimisation des données.

Au regard des dispositions du code du travail et de la réglementation sur la protection des données personelles, toutes les informations que le travailleur a pu révéler dans le cadre des échanges ne doivent pas nécessairement intégrer son DMST. Seules celles considérées comme utiles à son suivi et à la poursuite des missions du SPST par les professionnels de santé peuvent être enregistrées et conservées.

Par exemple, les informations touchant à l'intimité de la vie privée (religion, orientation sexuelle, opinions politiques, etc.) n'apparaissent en principe pas nécessaires au SPST pour exercer ses missions. Ainsi, sauf circonstances particulières le justifiant (p. ex. : travailleur faisant l'objet de discrimination fondée sur l'un de ces éléments, qu'il soit réel ou supposé), elles ne doivent en principe pas faire l'objet d'une conservation et ne peuvent donc être inscrites dans le DMST.

À l'inverse, certaines situations particulières peuvent justifier que d'autres informations que celles rappelées dans le tableau ci-dessus soient collectées (p. ex., la vérification de l'obligation vaccinale pour les professionnels de santé, la prévention des addictions, la charge mentale particulièrement importante d'un travailleur).

Le SPST doit également veiller au niveau de détail des informations inscrites dans le DMST. Par exemple, si le travailleur fait face à des relations conflictuelles avec certains de ses collègues, l'inscription de l'identité des autres travailleurs dans le DMST n'apparaît en principe pas utile.

Le principe de minimisation implique également qu'en cas de communication des données (p. ex.: au Groupe d'alerte en santé travail – GAST), seules celles étant essentielles à l'objectif poursuivi par la transmission soient communiquées. Le SPST doit donc effectuer un tri entre les informations, afin de ne transmettre que celles étant pertinentes et d'un niveau de détail adapté.

Les professionnels doivent être très vigilants dans l'utilisation des informations contenues dans le DMST, qui constitue, pour l'essentiel, des données de santé.

En vertu de la réglementation, ces données sont particulièrement sensibles. Elles font l'objet d'une protection toute particulière au même titre que les informations révélant la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ou encore l'orientation sexuelle. Elles **ne peuvent en principe pas être traitées, sauf exceptions prévues par les textes**.

Le SPST doit donc veiller à ne traiter des données de santé des travailleurs, dans le DMST, que sur la base de l'exception prévoyant que le fichier « *est* ***nécessaire aux fins de la médecine préventive ou de la médecine du travail****, de l'appréciation de la capacité de travail du travailleur* ».

Durée de conservation du DMST

Le code du travail prévoit une durée de conservation du DMST de quarante ans à compter de la date de la dernière visite ou examen du travailleur au sein du SPST concerné, dans la limite d'une durée de dix ans à compter du décès de la personne.

Par exception pour les travailleurs susceptibles d'être exposés à des risques particuliers, il existe dans le code du travail des règles spécifiques imposant une durée de conservation du DMST plus longue. Le tableau ci-dessous recense les différentes durées de conservation à appliquer aux dossiers médicaux des travailleurs exposés à des risques particuliers.

Nature du risque	Durée de conservation des informations
Agents biologiques pathogènes (art. R. 4426-9 du code du travail)	Conservation du dossier médical pendant une durée pouvant aller jusqu'à 40 ans, après la cessation de l'exposition connue
Agents chimiques dangereux et amiante (art. R. 4412-55 du code du travail)	Conservation du dossier médical durant 50 ans, après la fin de la période d'exposition
Rayonnements ionisants (art. R. 4451-83 du code du travail)	Conservation du DMST jusqu'au moment où le travailleur a ou aurait atteint l'âge de 75 ans et, en tout état de cause, pendant une période d'au moins 50 ans après la fin de la période d'exposition

Mesures de sécurité applicables au DMST

Afin de garantir l'échange, le partage, la sécurité et la confidentialité des informations relatives à la santé des travailleurs dans leur DMST, les systèmes d'information, les services ou les outils numériques destinés à être utilisés par les professionnels de santé exerçant au sein des SPST doivent être conformes aux règles d'identification électronique et aux référentiels d'interopérabilité et de sécurité élaborés par l'Agence du numérique en santé.

› Pour plus d'informations, voir l'arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé.

Attention

Si le DMST est conservé par un prestataire extérieur, les dispositions sur l'hébergement de données de santé s'appliquent (art. L. 1111-8 et R. 1111-8-8 et suivants du code de la santé publique). Le prestataire choisi devra être certifié hébergeur de données de santé (ou agréé selon la réglementation applicable).

Pour consulter la liste des hébergeurs de données de santé, voir « Liste des hébergeurs agréés » sur esante.gouv.fr

Les recommandations de la CNIL en matière de mot de passe doivent être respectées.

Les questions à se poser

- De quelles informations le professionnel de santé du SPST a-t-il vraiment besoin pour prévenir une altération de l'état de santé du travailleur et assurer son suivi ?
- Une procédure de gestion des habilitations et des accès est-elle mise en place ? Les professionnels peuvent-ils accéder, au regard de leurs missions, aux informations recueillies dans le DMST ?
- Les durées de conservation prévues par le code du travail (art. R. 4412-55, R. 4426-9, R.4451-83, R.4624-45-9) sont-elles respectées ?
- Les mesures mises en place pour assurer la sécurité et la confidentialité des données personnelles contenues dans le DMST sont-elles conformes à la règlementation sur la protection des données personnelles et aux référentiels d'interopérabilité et de sécurité élaborés par l'Agence du numérique en santé ?

POUR ALLER PLUS LOIN

- Article 5 du RGPD (principes), cnil.fr
- Article 32 du RGPD (sécurité du traitement), cnil.fr
- Article 35 du RGPD (analyse d'impact relative à la protection des données), cnil.fr
- Articles L. 1111-15 et s. du code de la santé publique (information à indiquer dans le dossier médical partagé)
- Articles L. 4624-8 et s. et R. 4412-55, R. 4426-9, R.4451-83, R.4624-45-9 du code du travail (dossier médical partagé)
- « Le dossier médical en santé au travail. Recommandation de bonne pratique », has-sante.fr
- Guide sur la sécurité des données personnelles – édition 2023 (PDF, 641 ko), cnil.fr

FICHE N° 11 : QUI PEUT ALIMENTER ET ACCÉDER AUX DONNÉES PERSONNELLES CONTENUES DANS LE DOSSIER MÉDICAL EN SANTÉ AU TRAVAIL ?

Règles de droit

L'ensemble des données personnelles des travailleurs concernant leur état de santé et leurs conditions de travail sont, pour l'essentiel, inscrites dans le dossier médical en santé au travail (DMST) tenu par le service de prévention et de santé au travail (SPST). Ce dossier retrace, dans le respect du secret médical, les informations relatives à l'état de santé du travailleur, aux expositions auxquelles il a été soumis ainsi que les avis et propositions du médecin du travail concernant notamment les mesures individuelles d'aménagement, d'adaptation ou de transformation du poste.

Les **informations portant sur l'état de santé des travailleurs sont considérées comme particulièrement sensibles**. Elles impliquent d'appliquer des mesures particulières pour leur utilisation, notamment d'accomplir, dans certaines situations, des formalités auprès de la CNIL.

› Pour plus d'informations, nous vous invitons à consulter les fiches n°9 et n° 12.

La règle du secret médical impose à la direction du SPST de formaliser une procédure pour définir la gestion des habilitations et des accès, sous l'autorité du médecin du travail.

Cette procédure doit permettre l'accessibilité au DMST exclusivement dans le cadre d'un accès autorisé, sous peine de voir la transmission des données qualifiée de violation de données. Au plan technique, elle doit inclure des mesures garantissant la sécurité et la confidentialité des informations.

› Pour plus d'informations, voir :
- « Les violations de données personnelles », cnil.fr
- Le guide pratique consacré aux tiers autorisés (PDF, 720 ko), cnil.fr

Le code du travail (article R.4624-45-5) encadre strictement les modalités d'alimentation et de consultation du DMST par les professionnels du SPST.

En pratique

En quoi consiste la gestion des habilitations et des accès pour le DMST ?

Qui en est responsable ?

Au sein du SPST, les **personnes autorisées à alimenter et à accéder aux données personnelles collectées dans le DMST doivent être identifiées ainsi que l'étendue de leur accès**, en tenant compte de leurs compétences et de la nature des missions exercées par chacun des professionnels. Toutes ces personnes ne disposent pas des mêmes droits.

Le SPST étant juridiquement responsable de traitement, sa direction est responsable de l'application des règles en la matière. Elle doit s'assurer que les mesures mises en place présentent toutes les garanties requises par la réglementation.

Attention

Cela ne signifie pas que le médecin du travail ne dispose d'aucune compétence particulière concernant la gestion du DMST. Bien au contraire, la Haute Autorité de santé (HAS) recommande que la gestion des accès soit assurée par le médecin du travail, qui endosse le rôle d' « administrateur du logiciel ».

Par ailleurs, d'après l'article R. 4127-72 du code de la santé publique, le médecin doit veiller à ce que les personnes qui l'assistent dans son exercice soient instruites de leurs obligations en matière de secret professionnel et s'y conforment. Par conséquent, la mise en œuvre opérationnelle de la politique de gestion des habilitations et des accès des professionnels de santé et des autres membres de l'équipe pluridisciplinaire du SPST est en principe assurée par le médecin du travail.

Une solution est par exemple d'attribuer au médecin du travail l'administration des droits ou de prévoir que son accord sera automatiquement requis pour prendre toute décision en matière de gestion des habilitations et des accès au DMST. Par ailleurs, le médecin du travail doit signaler à la direction du SPST toute mesure prise ou toute situation susceptible de ne pas être conforme aux règles entourant le secret professionnel, par exemple si l'employeur accède au DMST. Il doit également veiller quotidiennement au strict respect des mesures prises, en contrôlant par exemple le respect de la confidentialité des mots de passe personnels.

Qui accède à quoi dans le DMST ? Qui peut l'alimenter ?

Seuls les professionnels de santé du SPST peuvent consulter et alimenter l'ensemble du DMST.

Les autres membres de l'équipe pluridisciplinaire, placés sous la supervision du médecin du travail, ne peuvent quant à eux consulter et alimenter que certaines parties du DMST.

Attention

Tous les membres de l'équipe pluridisciplinaire ne disposent pas des mêmes droits.

Seuls les professionnels de santé accèdent à l'ensemble des données présentes dans le DMST. Il en est donc ainsi des infirmiers, des collaborateurs médecins, des médecins du travail, des médecins praticiens correspondants ou internes en médecine des SPST. À noter que le travailleur peut s'opposer à l'accès au DMST du médecin correspondant ou des professionnels de santé chargés d'assurer, sous l'autorité du médecin du travail, le suivi de son état de santé.

Les autres membres de l'équipe pluridisciplinaire (notamment ergonomes, toxicologues, assistants de service de santé au travail) ne sont pas autorisés à accéder à l'ensemble des informations contenues dans le DMST. Ces professionnels ne sont autorisés à accéder qu'aux données suivantes : identité du travailleur, données médico-administratives nécessaires à la coordination de sa prise en charge (identifiant national de santé notamment), données d'identité et de contact de son médecin traitant, informations sur les risques actuels ou passés du travail. Cet accès s'effectue sur délégation du médecin du travail et sous sa responsabilité. Les mêmes règles s'appliquent à l'alimentation du DMST par ces professionnels.

Les travailleurs sociaux rattachés à un SPST, et n'appartenant pas à l'équipe pluridisciplinaire, ne peuvent par conséquent ni alimenter, ni accéder au DMST.

Au regard de leurs compétences et de leurs missions, **le personnel de direction** (directeurs, sous-directeurs, etc.) et, plus généralement, **le personnel administratif** (agents en charge des ressources humaines, de la comptabilité, etc.) **ne sont pas autorisés à prendre connaissance du contenu du DMST des travailleurs**.

Lorsqu'un travailleur relève de plusieurs SPST ou cesse de relever d'un SPST, le SPST compétent en charge de la continuité du suivi individuel du travailleur peut demander la transmission de son DMST, sauf dans l'hypothèse où le travailleur a déjà exprimé son opposition à une telle transmission.

Attention

Dans cette hypothèse, le SPST demandeur informe le travailleur et s'assure que ce dernier ne s'oppose pas à une telle transmission.

FOCUS

Le dispositif d'accès et de partage des informations contenues dans le dossier médical partagé (DMP) et le DMST

La loi n° 2021-1018 du 2 août 2021 reconnaît la contribution de la santé au travail à la santé publique. Elle prévoit un dispositif d'accès et de partage des informations contenues dans le DMP et le DMST.

À compter du 1er janvier 2024, le DMP comporte un volet relatif à la santé au travail dans lequel sont versés les éléments du DMST du travailleur, nécessaires au développement de la prévention ainsi qu'à la coordination, à la qualité et à la continuité des soins.

Ce volet ne peut être complété que si le travailleur, préalablement informé, a donné son consentement. Les catégories d'informations susceptibles d'y être collectées sont définies par la HAS, dans le cadre des recommandations de bonnes pratiques du 16 mars 2023.

Le médecin du travail chargé du suivi de l'état de santé du travailleur peut accéder à son DMP et alimenter le volet relatif à la santé au travail, sous réserve que le travailleur donne son consentement exprès après avoir été informé préalablement de sa possibilité de restreindre l'accès au contenu de son DMP.

Le travailleur peut s'opposer à l'accès du médecin du travail chargé du suivi de son état de santé à son DMP. Ce refus ne constitue pas une faute et n'est pas porté à la connaissance de l'employeur.

Le volet relatif à la santé au travail du DMP est accessible, uniquement à des fins de consultation, aux professionnels de santé appartenant à l'équipe de soins participant à la prise en charge habituelle du travailleur (en dehors du contexte professionnel), à la condition que le travailleur préalablement informé y consente.

L'employeur peut-il accéder au DMST du travailleur ?

L'employeur est exclu de la liste des personnes autorisées par le code du travail à obtenir communication du DMST.

Attention

L'interdiction pour un employeur d'accéder au DMST est un principe fondamental. En effet, le médecin du travail reste indépendant de l'employeur dans l'exercice de ses missions et est tenu au secret médical, y compris lorsqu'il exerce au sein d'un SPST autonome implanté dans les locaux de l'employeur. Il est responsable du contenu des dossiers médicaux et doit veiller à ce que la confidentialité des informations soit préservée. En particulier, conformément à l'article R. 4127-72 du code de la santé publique, il doit veiller à ce que les personnes qui l'assistent soient instruites de leurs obligations en matière de secret professionnel et s'y conforment.

› Pour plus d'informations, voir la fiche n°2 relative aux responsabilités de traitement et la fiche n° 8 relative à la sécurité des informations.

En revanche, le médecin du travail peut adresser à l'employeur, dans le respect des dispositions du code du travail, des propositions ou faire des préconisations découlant du suivi médical du travailleur pour aménager ses conditions de travail. L'employeur ne doit cependant pas recevoir communication des informations médicales justifiant la mise en place de telles mesures individuelles.

Exemple

Peuvent être communiqués :

- l'avis d'aptitude ou d'inaptitude rendu conformément aux dispositions de l'article L. 4624-4 du code du travail dans le cadre du suivi individuel renforcé du travailleur ;
- les mesures individuelles d'aménagement, d'adaptation ou de transformation du poste de travail ou des mesures d'aménagement du temps de travail justifiées par des considérations relatives notamment à l'âge ou à l'état de santé physique et mentale du travailleur ;
- les préconisations émises en matière de reclassement du travailleur.

Les questions à se poser

- Une procédure encadrant les modalités de définition de la politique de gestion des habilitations et des accès conforme aux compétences et missions des professionnels exerçant au sein du SPST est-elle mise en place ?
- Le médecin du travail a-t-il été associé à l'élaboration de cette politique ?
- Quel est le rôle du médecin du travail dans la mise en œuvre au quotidien de cette politique ?
- Les travailleurs sont-ils informés que les employeurs sont destinataires de certaines informations découlant de leur suivi médical telles que les avis d'aptitude ou d'inaptitude mais qu'ils ne disposent d'aucun droit d'accès au DMST ?

- Les travailleurs sont-ils informés de leur droit de s'opposer, selon des modalités prévues à l'article R. 4624-45- 6 du code du travail, à l'accès à leur DMST par les professionnels de santé autres que le médecin du travail chargés d'assurer leur suivi ?
- Des mesures de sécurité particulières sont-elles mises en place pour sécuriser les échanges entre les professionnels habilités du SPST ?
- Une procédure d'information et de recueil du consentement des travailleurs est-elle mise en place concernant les règles applicables au « volet santé au travail » du DMP ?
- Quelles informations du DMST est-il nécessaire d'intégrer dans le volet « santé au travail » du DMP (si le travailleur a donné son accord) ?

POUR ALLER PLUS LOIN

- Article 5 du RGPD (principes), cnil.fr
- Article 32 et suivants du RGPD (sécurité du traitement), cnil.fr
- Articles L. 4622-4, L. 4624-8 et R. 4624-10 et suivants du code du travail (services de prévention et de santé au travail), legifrance.gouv.fr
- Article R. 4127-5 et R. 4127-95 du code de la santé publique (médecine du travail sur legifrance.gouv.fr)
- Guide sur la sécurité des données personnelles – édition 2023 (PDF, 641 ko), cnil.fr
- Guide de la CNIL sur les tiers autorisés – 2020 (PDF, 720 ko), cnil.fr
- « Recommandations de la HAS portant sur les catégories d'informations susceptibles d'être intégrées dans le volet santé au travail du dossier médical partagé », has-sante.fr

FICHE N° 12 : ÉTUDES ET ENQUÊTES RÉALISÉES AU SEIN DU SPST : QUEL CADRE JURIDIQUE FAUT-IL APPLIQUER ?

Règles de droit

Les médecins du travail et autres professionnels de santé s'interrogent régulièrement sur **le lien entre les pathologies observées sur les travailleurs et leurs conditions de travail**.

Aussi mènent-ils ou participent-ils, à l'échelle d'une entreprise ou au niveau local, régional ou national, à des **recherches**, des **études**, des **évaluations** et des **enquêtes** (désignées ci-après sous le terme d'études), leur permettant de fournir des indicateurs en santé au travail, d'identifier des affections pouvant être provoquées ou aggravées par une activité professionnelle, de déterminer les actions de santé au travail à mettre en œuvre pour préserver la santé physique et mentale des travailleurs.

L'utilisation de données personnelles (fichiers, bases de données), directement identifiantes ou indirectement identifiantes, à de telles fins dans le domaine de la santé fait l'objet d'**un encadrement juridique particulier**.

Attention

Dans l'hypothèse – cependant **relativement rare en pratique** – où les données personnelles utilisées pour les études, évaluations ou enquêtes seraient anonymes, celles-ci n'entreraient pas dans le champ de la réglementation sur la protection des données personnelles.

L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible. Elle ne doit pas être confondue avec la pseudonymisation qui est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique, sans information supplémentaire.

Pour déterminer si les données sont anonymes ou pseudonymes, il est possible de se rapprocher de son délégué à la protection des données (s'il a été désigné).

Pour plus d'informations sur l'anonymisation :

- « L'anonymisation de données personnelles », cnil.fr
- L'avis du Comité européen de la protection des données n° 05/2014 du 10 avril 2014 (PDF, 855 ko), ec.europa.eu

Selon le périmètre et la nature de ces études, **certaines formalités devront être réalisées auprès de la CNIL** préalablement à leur mise en œuvre, par le responsable de traitement (p. ex. : le SPST ou encore l'établissement de santé souhaitant mener une recherche sur l'origine professionnelle d'une maladie particulière).

Ainsi, l'utilisation de données personnelles sur la santé des travailleurs pour mener des études relevant du champ des missions des SPST doit **respecter les articles 72 et suivants de la loi Informatique et Libertés dédiés à la recherche en santé**. Tel sera le cas par exemple, pour une étude portant sur l'influence d'une pathologie sur le parcours professionnel des travailleurs, sur les effets de certains matériaux sur la santé et la sécurité des travailleurs, sur le maintien dans l'emploi des travailleurs en situation de handicap, ou encore sur les troubles musculo-squelettiques. Si les fichiers concernés ne comportent pas de données personnelles sur la santé des travailleurs, les articles relatifs à la recherche en santé ne s'appliqueront pas.

Attention

Il conviendra de bien identifier la responsabilité de traitement (responsabilité du fichier, de la base de données, etc.) dans le cas des études menées, dans la mesure où les obligations pèsent sur celui-ci. Selon les cas de figure, le responsable de traitement peut être le SPST, un établissement ou professionnel de santé, le comité social et économique, etc.

› Pour plus d'informations sur la responsabilité de traitement, voir la fiche n° 2.

La présente fiche **ne s'attache pas aux particularités des recherches impliquant la personne humaine, qui semblent peu courantes au sein des SPST**. Elle se focalise donc sur les études qualifiées de « recherches n'impliquant pas la personne humaine » (RNIPH), par exemple menées à partir des données personnelles figurant dans les DMST.

› Pour avoir une vue d'ensemble des différentes catégories de recherches, voir la fiche thématique « Recherche médicale : quel est le cadre légal ? » sur cnil.fr

En pratique

Avant de lancer des études, il convient d'identifier leur périmètre afin d'apprécier la nécessité de réaliser des formalités auprès de la CNIL ainsi que la nature des informations à délivrer.

Pour définir les formalités à accomplir, deux cas de figure doivent ainsi être distingués, selon le périmètre de l'étude :

1. L'étude est « interne » au SPST.

L'étude est « interne », si elle est menée **cumulativement** :
- à partir **des informations recueillies dans le cadre du suivi du travailleur** ;
- par les **personnels assurant ce suivi** (médecin du travail, collaborateur médecin, interne, du service de prévention et de santé au travail, etc.) ;
- pour leur **usage exclusif**.

Exemple d'étude interne

Une étude menée par le médecin du travail ou tout autre professionnel de santé du SPST portant sur les risques professionnels d'une entreprise déterminée (ex : lombalgie, chute, parallélisme des formes, exposition à des maladies), à partir des informations inscrites dans le DMST des travailleurs suivis par l'un des professionnels de santé du SPST, pour mettre en place des actions préventives.

Quelles actions accomplir ?

- **Aucune formalité** auprès de la CNIL n'est nécessaire dans la mesure où l'article 65 de la loi Informatique et Libertés exclut du champ des formalités préalables « *les traitements permettant d'effectuer des études à partir des données recueillies en application du 1° de l'article 44 de la présente loi lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif* ». Ce fichier devra en revanche être mentionné dans le registre des activités de traitement.
- **Une information auprès des travailleurs concernés** pour les informer de la réutilisation de leurs données à des fins de recherche doit être réalisée. Une note d'information individuelle sur l'étude doit être remise préalablement à sa réalisation, afin que les personnes concernées puissent s'y opposer. L'information individuelle peut également être réalisée via une page web dédiée, dont la personne a été préalablement informée (notamment via la remise d'un document à l'occasion d'une visite).

Quelle durée de conservation retenir ?

Les données personnelles relatives aux travailleurs se prêtant à la recherche et professionnels intervenant dans la recherche sont conservées pendant une durée définie par le responsable de traitement en base active et en archivage intermédiaire. Cette durée ne **doit pas excéder celle nécessaire à la réalisation des objectifs** de l'étude et doit être justifiée par le responsable de traitement.

› Pour plus d'informations sur la durée de conservation des données, voir la fiche n° 5.

2. L'étude est multicentrique ou implique que des données personnelles soient rendues accessibles à des personnes en dehors de l'équipe du SPST assurant le suivi individuel des travailleurs.

Exemples d'études multicentriques

- l'étude est menée à partir des informations recueillies auprès de l'ensemble des SPST présents au sein d'une même région ;
- des professionnels de santé non rattachés au SPST (les spécialistes d'une pathologie particulière exerçant au sein d'un établissement de santé, d'un centre de lutte contre le cancer, etc.) consultent les informations présentes dans les DMST pour mener une étude ;
- les informations du DMST sont appariées avec des informations présentes dans d'autres sources (questionnaires, dossier médical libéral, etc.).

Quelles actions accomplir ?

- Une **formalité** auprès de la CNIL est **nécessaire** :
  - le responsable de traitement est invité à mettre en œuvre son étude conformément aux référentiels dédiés aux recherches en santé n'impliquant pas la personne humaine (méthodologie de référence MR 004) et à réaliser un engagement de conformité à la **MR-004** auprès de la CNIL ;

- si le fichier n'est pas conforme à la MR-004, une demande d'autorisation doit être déposée par le responsable de traitement auprès de la plateforme des données de santé (avis CESREES + autorisation de la CNIL).

- **Une information individuelle portant sur le projet d'étude** devra être délivrée **auprès de chaque personne** dont les informations vont être utilisées :
  - il appartient au responsable de traitement d'informer les travailleurs concernés par l'étude. Dès lors, l'information peut être réalisée par le SPST intervenant pour le compte du responsable de traitement, sur la base d'un modèle défini par le responsable de traitement ;
  - à titre dérogatoire, notamment pour les recherches menées à partir des données personnelles présentes dans le DMST des travailleurs ayant quitté leur emploi, il est possible de ne pas informer individuellement le travailleur lorsque l'information se révèle impossible, exigerait des efforts disproportionnés ou compromettrait gravement la réalisation des objectifs de l'étude ;
  - dans cette hypothèse, des **mesures appropriées** devront être mises en place, notamment la diffusion de la note d'information sur le site web, un affichage systématique dans les locaux du SPST ou via la remise d'un document d'information à l'occasion d'une visite mentionnant qu'une réutilisation des données est possible dans le cadre d'études (le support renvoyant à une page web ou à des liens permettant d'accéder à une information), une communication au sein de l'entreprise, etc.

Attention

Pour être en conformité avec une MR, le responsable de traitement doit **notamment** :

- être en mesure de mettre en place une information individuelle sur le fichier utilisé pour la réalisation de l'étude, à destination de l'ensemble des personnes concernées ;
- n'utiliser que des **informations pseudonymisées** ou codées (pas de nom / prénom) des travailleurs pour son étude. Pour plus d'informations sur la notion de données pseudonymes, nous vous invitons à consulter le glossaire ;
- être en mesure de justifier la **pertinence scientifique** des informations qu'il utilise.

L'engagement de conformité à une MR est valable pour plusieurs recherches : il peut être réalisé pour l'ensemble des fichiers du SPST entrant dans le champ de la MR. Il faut être conforme en tous points à la MR.

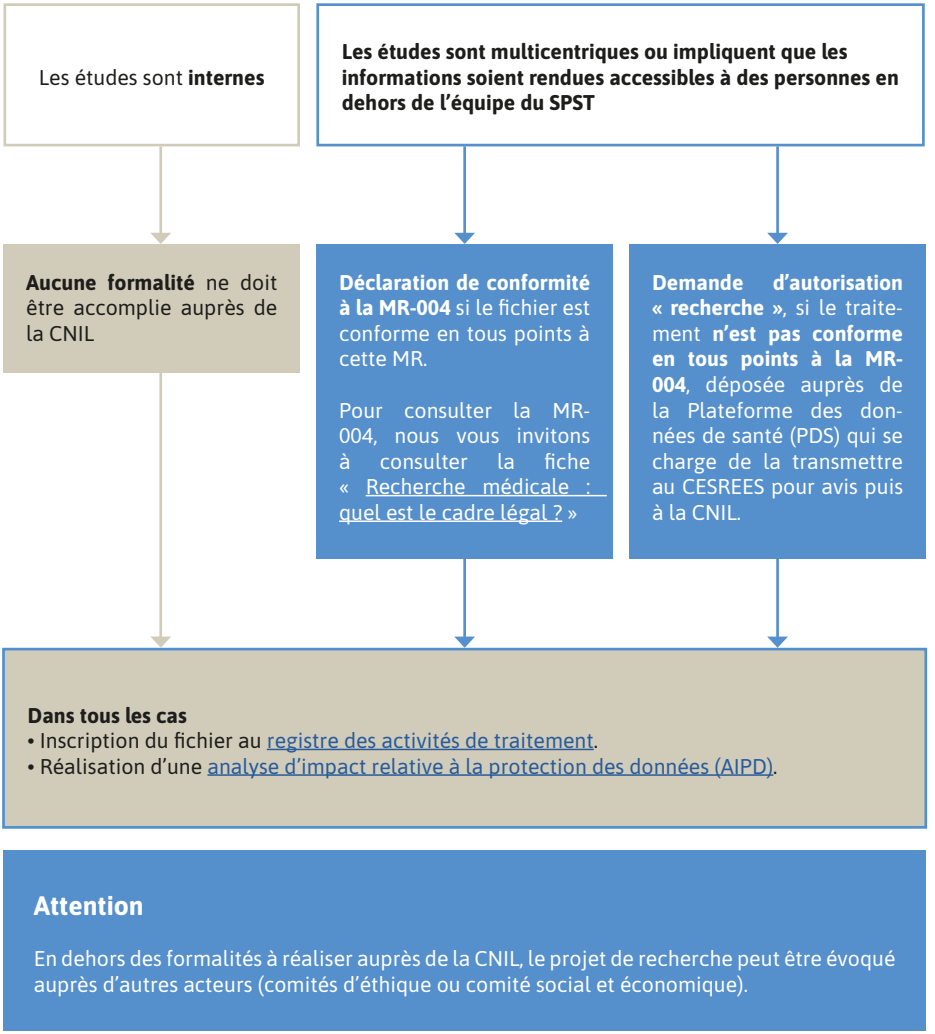
Si la recherche est conforme à la MR004, la saisine de la Plateforme des données de santé (PDS) ou de la CNIL n'est pas requise, mais des informations relatives à l'étude menée dans le cadre de ces MR devront être enregistrées dans le répertoire public de la PDS.

L'employeur et ses représentants n'ont pas à être informés que tel travailleur a participé, ou non, à une étude. L'employeur a accès aux résultats des études, sous réserve que ceux-ci ne permettent pas de réidentifier directement ou indirectement les travailleurs concernés.

› Pour plus d'informations sur la notion de données anonymes, voir le glossaire.

Le schéma ci-dessous synthétise les formalités applicables aux fichiers déployés au sein des SPST :

Quelles formalités accomplir auprès de la CNIL ?



Attention

En dehors des formalités à réaliser auprès de la CNIL, le projet de recherche peut être évoqué auprès d'autres acteurs (comités d'éthique ou comité social et économique).

Quelle durée de conservation retenir ?

Nature de la formalité	Nature des données	Durée de conservation en base active	Durée de conservation en archivage intermédiaire
Déclaration de conformité à la MR-004	Données personnelles concernant les travailleurs se prêtant à la recherche	Conservation dans les systèmes d'information du fichier, du centre participant ou du professionnel intervenant dans la recherche jusqu'à deux ans après la dernière publication En l'absence de publication : conservation jusqu'à la signature du rapport final de la recherche	Archivage sur un support papier ou informatique pour une durée conforme à la réglementation en vigueur ou pour une durée de 20 ans maximum
	Données personnelles concernant les professionnels intervenant dans la recherche	15 ans au maximum, à compter de la fin de la dernière recherche à laquelle les professionnels ont participé	Archivage sur support papier ou informatique pour une durée conforme à la réglementation en vigueur
Demande d'autorisation « recherche »	Données personnelles concernant les travailleurs se prêtant à la recherche et les professionnels intervenant dans la recherche	Conservation des informations des personnes concernées pendant une durée définie par le responsable de traitement et n'excédant pas celle nécessaire à la réalisation de la recherche	Archivage sur support papier ou informatique pour une durée conforme à la réglementation en vigueur

Les questions à se poser

- Qui est **responsable de traitement** (SPST, établissement de santé, autre) ?
- Quel est le **périmètre** de la recherche (recherche interne / recherche multicentrique) ?
- Quelle est la **nature** de la recherche (RNIPH / RIPH) ?
- L'**objectif** (la finalité) de la recherche est-il clairement défini ?
- Des **formalités** doivent-elles être accomplies auprès de la CNIL ?
- Les informations utilisées sont-elles **toutes strictement nécessaires** par rapport au sujet de la recherche ?
- Lorsque la recherche sera terminée, une **durée** à l'issue de laquelle les informations seront supprimées est-elle prévue ?
- Les travailleurs concernés seront-ils **informés** avant le début de la recherche ?
- L'ensemble des mentions obligatoires figure-t-il dans les notes d'information remises aux personnes concernées ?
- Le travailleur concerné pourra-t-il facilement **exercer ses droits** (droit d'accès, droit d'opposition, etc.) ?
- Les mesures mises en place sont-elles suffisantes pour préserver la **sécurité des données personnelles collectées** ?

- En cas de doute pour déterminer si les données sont anonymes ou pseudonymes l'avis du délégué à la protection des données a-t-il été demandé ?

POUR ALLER PLUS LOIN

- Article 9 du RGPD (données sensibles), cnil.fr
- Articles 72 et suivants de la loi Informatique et Libertés (traitements à des fins de recherche, étude ou évaluation en santé), cnil.fr
- Articles R. 4623-1 du code du travail (rôle de la médecine du travail), legifrance.gouv.fr
- Article R. 4624-1 du code du travail (missions des services de prévention et de santé au travail), legifrance.gouv.fr
- Article R. 4624-58 du code du travail (participation du médecin du travail aux recherches, études et enquêtes), legifrance.gouv.fr
- Articles L. 1121-1 du code du travail (droits des personnes au travail), legifrance.gouv.fr
- Article R.1121-1 du code de la santé publique (recherche médicales sur la personne humaine), legifrance.gouv.fr

FICHE N° 13 : QUELLES SONT LES RÈGLES APPLICABLES À LA TÉLÉSANTÉ AU TRAVAIL ?

Règles de droit

L'activité de télésanté, déployée par les SPST, constitue une pratique médicale nouvelle, réalisée à distance et utilisant les technologies de l'information et de la communication.

Elle met en rapport les professionnels de santé du SPST (médecin du travail, collaborateur médecin, interne en médecine du travail, infirmier) et le travailleur dans le cadre du suivi individuel de son état de santé. Elle permet que les visites et examens puissent s'effectuer à distance, par vidéotransmission, à l'initiative des professionnels de santé du SPST ou du travailleur.

Attention

La pertinence de la réalisation à distance d'une visite ou d'un examen, même sollicité par le travailleur, est appréciée par le professionnel de santé du SPST en charge du suivi de l'état de santé du travailleur.

Si le professionnel constate à distance qu'une consultation physique avec le travailleur ou qu'un équipement spécifique est nécessaire, une nouvelle visite est programmée en présence du travailleur dans les meilleurs délais et, le cas échéant, dans les délais prévus pour l'intervention des actes de suivi individuel de l'état de santé du travailleur.

L'acte de télésanté nécessite également le consentement préalable du travailleur.

En pratique

L'activité de télésanté entre dans le champ de la réglementation applicable en matière de protection des données personnelles (RGPD et loi Informatique et Libertés) pour le traitement de données personnelles réalisé via le dispositif de vidéotransmission utilisé.

Le SPST sera responsable de ce traitement. Pour plus d'informations, nous vous invitons à consulter la fiche n° 2.

À ce titre, le SPST doit garantir le respect des principes fondamentaux relatifs au traitement des données personnelles résultant de l'utilisation du dispositif de vidéotransmission, notamment en ce qui concerne :

- la finalité du traitement (voir la fiche n° 1) ;
- la nature des données collectées (voir la fiche n° 3) ;
- les durées de conservation (voir la fiche n° 5) ;
- les droits des personnes concernées (voir les fiches n° 6 et n° 7) ;
- les mesures de sécurité (voir la fiche n° 8).

Le SPST doit être en mesure de démontrer, à tout moment, sa conformité aux exigences du RGPD, en traçant toutes les démarches entreprises :

- la réalisation d'une AIPD ;
- la tenue du registre des activités de traitement ;
- l'information des travailleurs concernés, etc.

Pour plus d'informations, voir la fiche n° 9.

Attention

Le traitement de données personnelles utilisé pour la mise en œuvre des actes de télésanté via un dispositif de vidéotransmission, même s'il collecte des données de santé, ne fait l'objet d'aucune formalité particulière auprès de la CNIL.

Outre les garanties résultant de la réglementation sur la protection des données personnelles, le code du travail exige des garanties supplémentaires :

- Chaque visite ou examen effectué à distance nécessite de recueillir le consentement du travailleur à la réalisation de l'acte par vidéotransmission. Le cas échéant, le travailleur doit également consentir à ce que participe à cette visite ou à cet examen son médecin traitant ou un professionnel de santé de son choix.

Attention

Le consentement préalable du travailleur est recueilli par tout moyen il est consigné au sein de son DMST.

Si le travailleur ne consent pas à la réalisation à distance de la visite ou de l'examen, une consultation physique est programmée dans les meilleurs délais et, le cas échéant, dans les délais prévus pour les actes de suivi individuel de l'état de santé.

- Le professionnel de santé doit s'assurer que la visite ou l'examen en vidéotransmission peut être réalisé dans des conditions sonores et visuelles satisfaisantes et de nature à garantir la confidentialité des échanges.

Attention

Le traitement de données personnelles utilisé pour la mise en œuvre des actes de télésanté via un dispositif de vidéotransmission, même s'il collecte des données de santé, ne fait l'objet d'aucune formalité particulière auprès de la CNIL.

- Les dispositions du code de la santé publique (CSP) encadrant les services numériques en santé sont applicables à l'activité de télésanté déployé via un dispositif de vidéotransmission (article L. 1470-1 à 6 du CSP).

Les questions à se poser

- Les principes fondamentaux relatifs au traitement des données personnelles résultant de l'utilisation du dispositif de vidéotransmission sont-ils respectés ?
- La conformité au RGPD est-elle documentée ?
- En cas de difficultés liées à l'activité de télésanté, le délégué à la protection des données est-il informé et consulté ?

POUR ALLER PLUS LOIN

- Articles R. 4.624-41-1 et s. du code du travail (surveillance de l'état de santé des travailleurs), legifrance.gouv.fr
- Articles L. 1470-1 et s. du code de la santé publique (services numériques en santé), legifrance.gouv.fr
- Article 32 du RGPD (sécurité du traitement), cnil.fr
- Article 34 de la loi Informatique et Libertés (délai d'instruction des demande d'avis), cnil.fr

ANNEXE 1
TABLEAU DE SYNTHÈSE DES FINALITÉS DES TRAITEMENTS DE DONNÉES PERSONNELLES CONSTITUÉS PAR LES SPST

Activités	Finalités poursuivies
Activités liées à la qualité d'employeur du SPSTI	• En matière de ressources humaines : gestion du recrutement, gestion administrative du personnel, gestion de la paie, gestion des relations sociales • En matière comptable : gestion de la compatibilité fournisseurs, gestion des achats • En matière de sécurité des biens des personnes et des locaux • En matière de sécurité informatique • En matière de communication
Activités liées à la vie associative	• Gestion des mandats, gestion des désignations ou élections au conseil d'administration et à la commission de contrôle, gestion de l'assemblée générale, etc. • Gestion de l'agrément, des certifications du service, etc.
Activités liées à l'activité de prévention individuelle de la santé au travail des travailleurs	• Gestion de la relation adhérent (adhésion, facturation, etc.) • Gestion administrative des visites • Gestion de la prévention individuelle • Gestion du suivi individuel (dont tenue du DMST) • etc.
Activités liées à l'activité de prévention collective	Gestion des actions en milieu du travail (étude de poste, prélèvements, ateliers et sessions de formations des adhérents, sensibilisation saisonniers, etc.)
Activités d'études, recherches en santé, de la veille sanitaire et épidémiologique	

ANNEXE 2
CONDITIONS DE RÉUTILISATION DES DONNÉES PAR UN SPST

La réutilisation des données est **possible sous réserve de respecter l'objectif initial poursuivi lors de la collecte des données**. Les données recueillies pour un objectif déterminé **ne peuvent en effet pas être réutilisées pour un autre objectif qui serait incompatible**, c'est-à-dire fondamentalement différent ou sans lien avec le but initialement poursuivi par l'utilisation, sauf à démontrer sa « compatibilité ».

Exemple

La réutilisation des données ayant trait à la santé des travailleurs est compatible avec l'objectif de participer à des enquêtes épidémiologiques.

Pour s'assurer **de la compatibilité avec l'objectif initial, différents éléments** doivent être pris en considération :

- l'existence d'un lien éventuel entre l'objectif initial de l'utilisation des données et celui envisagé ;
- le contexte dans lequel les données sont collectées ;
- la nature des données personnelles recueillies (en particulier si des catégories particulières de données personnelles - informations de santé, informations relatives à l'appartenance syndicale, informations concernant la vie ou l'orientation sexuelle du travailleur - sont collectées) ;
- les conséquences possibles de l'utilisation ultérieure des données pour les personnes concernées (majoritairement les travailleurs) ;
- les garanties mises en place pour assurer la sécurité des informations, telles que le chiffrement des informations ou la pseudonymisation.

Attention

En cas de réutilisation des données pour une finalité ultérieure qui serait jugée compatible avec la finalité initiale, les professionnels intéressés du SPST devront en **informer le travailleur individuellement**, avant la mise en œuvre du nouveau fichier.

Pour répondre à cette obligation, il pourra être remis au travailleur un support mentionnant l'existence de pages web et/ou de liens permettant d'accéder à l'information et de s'opposer, le cas échéant, à la réutilisation de ses données.

En pratique, si le travailleur s'oppose à la réutilisation de ses données pour des raisons tenant à sa situation particulière, le SPST ne pourra pas en principe les utiliser pour cette nouvelle finalité, sauf s'il est en mesure de prouver un motif légitime et impérieux prévalant sur les intérêts et droits et libertés de la personne concernée malgré la demande de la personne concernée.

ANNEXE 3
MODÈLES DE FICHES DE REGISTRE DES ACTIVITÉS DE TRAITEMENT

Registre des activités de traitement mis en œuvre par [identité du responsable de traitement personnelles à compléter] Activité n° 1 : Gestion des dossiers médicaux en santé au travail	
Responsable de traitement	Service de prévention et de santé au travail
Coordonnées du délégué à la protection des données (DPO)	[Coordonnées du DPO à renseigner]
Objectifs du fichier	Gestion des dossiers médicaux en santé au travail
Base légale du fichier	Obligation légale
Catégories de personnes concernées	SPST autonomes : travailleurs exerçant au sein de l'organisme
Catégories des informations traitées	• les données d'identité et médico-administratives : nom, prénom, date de naissance, entreprise ou administration ; • les données d'identité et de contact du médecin traitant du travailleur ; • les informations permettant de connaître les risques auxquels le travailleur est ou a été exposé (ex : caractéristiques du ou des postes occupés ainsi que du secteur ; données d'exposition ; mesures de prévention mises en place) ; • les informations relatives à l'état de santé du travailleur recueillies lors des visites et examens (ex : certains antécédents médicaux ou tout autre élément de nature à caractériser l'état de santé du travailleur lorsqu'il nécessite un aménagement de poste) ; • les correspondances échangées entre professionnels de santé aux fins de la coordination et de la continuité de la prise en charge du travailleur ; • les informations formalisées concernant les attestations, avis et propositions des professionnels de santé au travail ; • la mention de l'information du travailleur sur ses droits en matière d'accès aux données le concernant et sur les conditions d'accès à son dossier médical de santé au travail ; • le consentement ou l'opposition du travailleur concernant le recours à des pratiques médicales ou de soins à distance en utilisant les technologies de l'information et de la communication ; • le consentement ou l'opposition du travailleur concernant l'accessibilité du dossier médical en santé au travail d'un autre SPST si le travailleur relève de plusieurs services.
Source des données	Pour les SPST autonomes : informations fournies par le travailleur concerné et l'employeur Pour les SPST interentreprises : informations fournies par le travailleur concerné et l'employeur

Registre des activités de traitement mis en œuvre par [identité du responsable de traitement personnelles à compléter] Activité n° 1 : Gestion des dossiers médicaux en santé au travail	
Caractère obligatoire ou facultatif du recueil des données et conséquences en cas de non-fourniture des données	Le SPST se trouve dans l'obligation de tenir un dossier de santé au travail. Le travailleur est libre de partager ou non des informations relatives à son état de santé avec les professionnels de santé du SPST
Accédants et destinataires des données	En fonction de leurs besoins respectifs, accèdent à tout ou partie des données : • l'employeur du travailleur pour les propositions d'aménagement par le médecin du travail ; • le Groupe d'alerte en santé travail. Pour plus d'informations, nous vous invitons à consulter la fiche n°4.
Transferts de données vers un pays hors Union européenne ou vers une organisation internationale	Le fichier ne prévoit pas de transferts de données hors Union européenne.
Prise de décision automatisée	Le fichier ne prévoit pas de prise de décision automatisée
Durée de conservation des données	[À renseigner par le responsable de traitement]. • Pour plus d'informations, nous vous invitons à consulter la fiche n°5.
Mesures de sécurité techniques / organisationnelles (description générale)	[À renseigner par le responsable de traitement]. • Pour plus d'informations, nous vous invitons à consulter la fiche n°8.
Source des données	• Droit d'accès • Droit de rectification • Droit à la limitation Pour plus d'informations, nous vous invitons à consulter la fiche n°7. Pour toute information ou aide dans l'exercice des droits, contacter le DPO
Droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL)	• Pour contacter la CNIL: https://www.cnil.fr/contact • Pour adresser une réclamation auprès de la CNIL : https://www.cnil.fr/plaintes
Rédacteur (s) de la fiche	[Fonction du (des) rédacteur(s) à renseigner]
Date de dernière mise à jour	[Date de la dernière mise à jour à renseigner]

Registre des activités de traitement mis en œuvre par [identité du responsable de traitement personnelles à compléter] Activité n° 2 : Gestion de la base de données des adhérents	
Responsable de traitement	Service de prévention et de santé au travail interentreprises
Coordonnées du délégué à la protection des données (DPO)	[Coordonnées du DPO à renseigner]
Objectifs du fichier	Gestion de la base de données des adhérents
Base légale du fichier	Intérêt légitime (Précision : le contrat ne peut pas fonder ce traitement car cette base légale suppose que la personne concernée soit partie au contrat, ce qui n'est pas le cas en l'espèce).
Catégories de personnes concernées	Personnes « contacts » au sein des entreprises adhérentes
Catégories des informations traitées	• Nom • Prénoms • Coordonnées de contact (téléphone, adresse électronique, adresse postale) • Entreprise ou administration concernée • Nombre de salariés au sein de l'entreprise ou de l'administration
Source des données	Entreprise ou administration adhérente
Caractère obligatoire ou facultatif du recueil des données et conséquences en cas de non-fourniture des données	Obligatoire
Catégories de destinataires des données	Membres du conseil d'administration paritaire du SPST interentreprises Membres du comité social et économique ou comité de contrôle en charge du contrôle du bon fonctionnement
Transferts de données vers un pays hors Union européenne ou vers une organisation internationale	Le fichier ne prévoit pas de transferts de données hors Union européenne.
Prise de décision automatisée	Non
Durée de conservation des données	Durée de la relation contractuelle
Mesures de sécurité techniques / organisationnelles (description générale)	

Registre des activités de traitement mis en œuvre par [identité du responsable de traitement personnelles à compléter] Activité n° 2 : Gestion de la base de données des adhérents	
Droits des personnes concernées	• Droit d'accès • Droit de rectification • Droit à l'effacement • Droit à la limitation • Droit d'opposition Pour toute information ou aide dans l'exercice des droits, contacter le DPO
Droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL)	• Pour contacter la CNIL: https://www.cnil.fr/contact • Pour adresser une réclamation auprès de la CNIL : https://www.cnil.fr/plaintes
Rédacteur (s) de la fiche	[Fonction du (des) rédacteur(s) à renseigner]
Date de dernière mise à jour	[Date de la dernière mise à jour à renseigner]

ANNEXE 4
MODÈLE DE NOTICE D'INFORMATION À UTILISER POUR LA GESTION DU DOSSIER MÉDICAL EN SANTÉ AU TRAVAIL

N.B. : cet exemple doit être adapté aux spécificités du fichier envisagé.

Les informations recueillies via la fiche de renseignement remplie préalablement au rendez-vous médical puis lors des échanges avec les membres du SPST sont utilisées par [nom et coordonnées du responsable de traitement].

Pour quelles raisons vos données personnelles sont-elles utilisées ?

Les données personnelles sont utilisées pour :

- compléter, constituer et gérer le dossier médical de santé au travail ;
- permettre au SPST de rédiger la fiche d'entreprise qui est un document informant l'employeur des risques professionnels et des effectifs des travailleurs qui y sont exposés, ainsi que des moyens de prévention mis en œuvre ou préconisés que le service a mis en évidence.

La tenue du dossier médical en santé au travail ainsi que la rédaction de la fiche d'entreprise sont obligatoires.

Quelle est la durée de conservation des informations ?

Elles sont conservées en principe pendant 40 ans à compter de la dernière visite [à compléter].

Qui peut recevoir communication des informations ?

Seuls ont accès aux informations figurant dans votre dossier médical l'équipe du SPST, les Groupes d'alerte en santé travail, en charge d'organiser la réponse aux signalements d'événements sanitaires inhabituels survenant en milieu professionnel et le médecin inspecteur du travail [à compléter].

L'employeur peut également recevoir communication de certaines d'informations dans le respect du secret médical. Ainsi, il obtient communication des avis et propositions de mesures individuelles d'aménagement des conditions de travail que le SPST émet consécutivement à l'évaluation de l'état de santé du travailleur telles que les avis d'aptitude ou d'inaptitude, les mesures individuelles d'aménagement d'un poste. En revanche, il ne peut pas accéder aux éléments médicaux présents dans votre dossier médical justifiant les avis et propositions formulés par le SPST.

Quels sont vos droits et comment les exercer ?

Vous pouvez accéder aux données personnelles vous concernant, les rectifier ou exercer votre droit à la limitation de l'utilisation de vos données personnelles.

Pour toute question relative à la protection de vos données personnelles ou pour exercer vos droits, vous pouvez contacter le délégué à la protection des données (DPO) de [identité du responsable de traitement à mentionner] à l'adresse suivante : [courriel du DPO ou adresse postale à renseigner].

Pour plus d'informations sur l'utilisation de vos données personnelles, nous vous invitons à consulter notre politique de confidentialité disponible à l'adresse suivante : [adresse de la politique de confidentialité du site web du SPST ou de l'employeur]
Si vous estimez, après avoir contacté [nom du responsable de traitement], que vos droits Informatique et Libertés ne sont pas respectés, vous pouvez adresser une réclamation en ligne à la CNIL .

NB : en parallèle, si l'employeur dispose d'un intranet dans lequel sont répertoriés l'ensemble des documents relatifs à la gestion des ressources humaines, un item relatif à la santé au travail pourrait utilement intégrer les éléments d'information relatifs à l'utilisation des données personnelles dans ce cadre.

ANNEXE 5
CAHIER DES CHARGES POUR ÉVALUER LA CONFORMITÉ DU DMST AU RGPD

Attention

La solution logicielle utilisée pour gérer le DMST devra permettre au SPST, en tant que responsable de traitement, de respecter les éléments du cahier des charges présenté ci-dessous.

Identification des acteurs	OUI	NON
Le SPST est-il identifié comme responsable de traitement pour la gestion du DMST ?		
Existe-t-il un ou plusieurs sous-traitant pour gérer le DMST ?		
Avant de choisir un sous-traitant pour le DMST, le SPST a-t-il vérifié que celui-ci présentait des garanties suffisantes aux plans technique et organisationnel pour que le DMST soit conforme aux exigences du RGPD ?		
Un contrat de sous-traitance conforme aux exigences de l'article 28 du RGPD est-il passé ?		
Est-ce qu'un prestataire extérieur assure la conservation du DMST ?		
Dans l'affirmative, ce prestataire est-il certifié hébergeur de données de santé (ou agréé selon la réglementation applicable) conformément aux dispositions de l'article L. 1111-8 du code de la santé publique ?		
Finalité du DMST	**OUI**	**NON**
La finalité du DMST est-elle clairement identifiée ?		
Les informations collectées dans le DMST par les professionnels de santé assurant le suivi du travailleur et les autres professionnels de l'équipe pluridisciplinaire sont-elles collectées pour des usages déterminés (définis avec précision), explicites (clairs et compréhensibles pour le travailleur) et légitimes (c'est-à-dire ne portant pas atteinte à la réglementation ou à une liberté fondamentale) ?		
Identification de la base légale du DMST	**OUI**	**NON**
Ce qui justifie que le SPST soit autorisé à créer un DMST sur chaque travailleur : Est-ce une obligation légale ?		
Nature des données personnelles collectées dans le DMST	**OUI**	**NON**
Quelles sont les données personnelles susceptibles d'être recueillies dans le DMST du travailleur ? (liste à produire)	Non adapté	
Les données personnelles recueillies dans le DMST sont-elles adéquates, pertinentes et nécessaires ?		

Les données personnelles recueillies dans le DMST sont -elles exactes et peuvent-elles être mises à jour ?		
Information des personnes concernées	**OUI**	**NON**
Les travailleurs suivis par le SPST et les professionnels habilités à alimenter le SPST sont-ils informés que des données personnelles les concernant sont collectées et conservées dans le DMST ?		
Comment les travailleurs sont-ils informés que des données personnelles les concernant sont collectées et conservées dans le DMST ?	Non adapté	
L'information porte-t-elle sur l'ensemble des caractéristiques essentielles du DMST (objectif, nature des données collectées, durée de conservation, etc.) ?		
Échange et partage des données du DMST	**OUI**	**NON**
L'outil permet-il de distinguer plusieurs niveaux d'accès aux données contenues dans le DMST ?		
Quelles informations du DMST sont échangées et partagées ?	Non adapté	
A-t-on identifié avec qui les données du DMST peuvent être échangées et partagées (procédure de gestion des habilitations et des accès) ?		
A-t-on identifié comment le partage et l'échange de données intervient (règles de partage et d'échange) ?		
Les personnes qui reçoivent communication des données sont-elles bien autorisées à alimenter ou accéder au DMST au regard de leurs compétences et de leurs missions (procédure de gestion des habilitations et des accès) ?		
Les personnes sont-elles bien autorisées à accéder aux données du DMST au regard de leurs compétences et de leurs missions (procédure de gestion des habilitations et des accès) ?		
Modalités d'exercice des droits	**OUI**	**NON**
Les travailleurs peuvent-ils exercer leurs droits (accès, rectification, etc.) ?		
Un outil permet-il au SPST de répondre aisément aux demandes de droit d'accès ? (ex : bouton permettant d'extraire l'ensemble des données du DMST d'un travailleur)		
Les travailleurs sont-ils informés des modalités d'exercice de leurs droits ?		
Réutilisation des données du DMST dans le cadre des recherches, études et enquêtes	**OUI**	**NON**
Une réutilisation des données du DMST par le SPST ou des acteurs extérieurs au SPST est-elle prévue pour réaliser des recherches, études et enquêtes ?		
Le responsable de traitement du fichier ou de la base de données utilisé pour mener la recherche à partir des données personnelles du DMST est-il identifié ?		
Une vérification de la conformité de la recherche aux exigences du RGPD est-elle menée par le SPST, préalablement à l'accès aux données personnelles contenues dans le DMST ?		
Les dispositions particulières de la loi Informatique et Libertés applicables aux études, recherches et évaluations sont-elles respectées ?		

Durée de conservation du DMST	OUI	NON
La durée de conservation des données prévue par le code du travail pour le DMST est-elle appliquée ?		
Les travailleurs sont-ils informés de cette durée de conservation ?		
À l'issue de cette durée de conservation, qu'est-il prévu pour le DMST ? • Les données du DMST sont-elles détruites ? • Les données du DMST sont-elles anonymisés ?		
Mesures de sécurité	**OUI**	**NON**
Authentification des utilisateurs • Un identifiant (login) unique à chaque utilisateur a-t-il été défini ? • Une politique de mots de passe utilisateur conforme aux recommandations de la CNIL a-t-elle été adoptée ? • L'utilisateur a-t-il l'obligation de changer son mot de passe après réinitialisation ? • Le nombre de tentatives d'accès à un compte est-il limité ?		
Gestion des habilitations • Les profils d'habilitation sont-ils définis ? • Les permissions d'accès obsolètes sont-elles supprimées ? • Une revue annuelle des habilitations est-elle réalisée ?		
Traçabilité des accès et gestion des incidents • Un système de journalisation est-il prévu ? • Les utilisateurs sont-ils informés de la mise en place du système de journalisation ? • Les équipements de journalisation et les informations journalisées sont-ils protégés ? • Des procédures pour les notifications de violation de données personnelles sont-elles prévues ?		
Sécurisation des postes de travail • Une procédure de verrouillage automatique de session est-elle prévue ? • Des antivirus régulièrement mis à jour sont-ils utilisés ? • Une « pare-feu » (firewall) logiciel est-il utilisé ? • L'accord de l'utilisateur avant toute intervention sur son poste est-il recueilli ?		
Sécurisation de l'informatique mobile • Des moyens de chiffrement des équipements mobiles sont-ils prévus ? • Est-il procédé à des sauvegardes ou synchronisations régulières des données ? • Un secret pour le déverrouillage des smartphones est-il exigé ?		
Protection du réseau informatique interne • Les flux réseau sont-ils limités au strict nécessaire ? • Les accès distants des appareils informatiques nomades par VPN sont-ils sécurisés ? • Le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi est-il mis en oeuvre ?		
Sécurisation des serveurs • L'accès aux outils et interfaces d'administration aux seules personnes habilitées est-il limité ? • Les mises à jour critiques sont-elles installées sans délai ? • Une disponibilité des données est-elle assurée ?		
Sécurisation des sites web • Le protocole TLS est-il utilisé ? Sa mise en œuvre est-elle vérifiée ? • A-t-on vérifié qu'aucun mot de passe ou identifiant ne passe dans les URL ? • A-t-on contrôlé que les entrées des utilisateurs correspondent à ce qui est attendu ? • Un bandeau de consentement pour les cookies non nécessaires au service a-t-il été mis ?		

Sauvegarde et continuité de l'activité • Des sauvegardes régulières sont-elles effectuées ? • Les supports de sauvegarde sont-ils stockés dans un endroit sûr ? • Des moyens de sécurité pour le convoyage des sauvegardes sont-ils prévus ? • La continuité d'activité est-elle prévue ? Est-elle testée de manière régulière ?		
Archivage sécurisé • Des modalités d'accès spécifiques aux données archivées sont-elles mises en oeuvre ? • Les archives obsolètes sont-elles détruites de manière sécurisée ?		
Encadrement de la maintenance et de la destruction des données • Les interventions de maintenance sont-elles enregistrées dans une main courante ? • Les interventions par des tiers sont-elles encadrées par un responsable de l'organisme ? • Les données de tout matériel sont-elles effacées avant sa mise au rebut ?		
Gestion de la sous-traitance • Une clause spécifique est-elle prévue dans les contrats des sous-traitants pour encadrer les obligations du sous-traitant ? • Les conditions de restitution et de destruction des données sont-elles prévues ? • A-t-on vérifié l'effectivité des garanties prévues (audits de sécurité, visites, etc.) ?		
Sécurisation des échanges avec d'autres organismes • Les données sont-elles chiffrées avant leur envoi ? • A-t-on vérifié qu'il s'agit du bon destinataire ? • Le secret est-il transmis lors d'un envoi distinct et via un canal différent ?		
Protection des locaux • Les accès aux locaux sont-ils restreints au moyen de portes verrouillées ? • Des alarmes anti-intrusion sont-elles installées ? Sont-elles vérifiées périodiquement ?		
Encadrement des développements informatiques • Des paramètres respectueux de la vie privée sont-ils proposés aux utilisateurs finaux ? • Les zones de commentaires sont-elles évitées ou sont-elles encadrées strictement ? • Les tests sont-ils réalisés sur des données fictives ou anonymisées ?		
Utilisation des fonctions cryptographiques • Des algorithmes, des logiciels et des bibliothèques reconnues sont-ils utilisés ? • Les secrets et les clés cryptographiques sont-ils conservés de manière sécurisée ?		
Actions menées pour apprécier la conformité au RGPD ?	**OUI**	**NON**
Un registre des activités de traitement est-il tenu ? • Comporte-t-il une fiche dédiée au DMST ?		
Une analyse d'impact relative à la protection des données a-t-elle été faite pour le DMST ?		
La conformité du DMST au RGPD est-elle documentée ?		
Un délégué à la protection des données a-t-il été désigné ? • A-t-il été sollicité pour répondre aux interrogations en lien avec le déploiement du DMST ?		

GLOSSAIRE

Analyse d'impact relative à la vie privée

Outil permettant d'analyser les risques d'un projet de traitement afin de les limiter pour construire un traitement respectueux de la vie privée.

Anonymisation

Technique permettant de rendre impossible l'identification de la personne concernée, qu'importe le moyen employé.

Archivage intermédiaire ou base intermédiaire

Base de données dont l'accès est particulièrement circonscrit car les informations ne sont pas nécessaires pour la gestion courante mais dont la conservation est importante pour l'organisme, pour se prémunir d'un éventuel contentieux par exemple.

Base active

Base de données permettant l'usage courant des données personnelles c'est-à-dire l'exploitation courante des données qui sont en conséquence aisément accessibles.

Confidentialité

Sécurisation des données afin que ces dernières ne fassent pas l'objet d'une divulgation.

Disponibilité

Sécurisation des données afin que ces dernières soient accessibles à tout moment.

Finalité

Objectif de l'utilisation de données personnelles, c'est-à-dire la raison pour laquelle le SPST manipule des données personnelles.

Habilitation

Droits octroyés à des personnes pour accéder aux informations dans un document, une base de données et/ou les modifier.

Information personnelle

(ou donnée personnelle ou donnée à caractère personnel)

Toute information se rapportant à une personne physique identifiée ou identifiable, même indirectement ou très difficilement.

Le sens des termes « information personnelle », « donnée à caractère personnel » et « donnée personnelle » y est équivalent.

Intégrité

Sécurisation des données afin que ces dernières ne soient ni altérées, ni détruites.

Intervenants en prévention des risques

Ce sont les psychologues, les toxicologues, les ergonomes, etc.

Pseudonymisation

Techniques permettant de ne plus être en mesure d'identifier la personne physique concernée par des données personnelles sans avoir recours à des informations supplémentaires.

Registre

Document permettant de recenser les traitements mis en œuvre de votre organisme ainsi que leurs caractéristiques afin de justifier de leur conformité au RGPD.

Traitement

Toute utilisation ou manipulation de données personnelles : collecte, conservation, transmission, modification, etc.

Commission nationale de l'informatique et des libertés
3, Place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
01 53 73 22 22

Novembre 2023

www.cnil.fr
linc.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr