Erwan TREHIOU
Avocat

CONSULTATION JURIDIQUE

Le RGPD et les Services de Santé au Travail Interentreprises

INTRODUCTION

1. Le Règlement 2016/679/UE du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « le RGPD ») est entré en vigueur le 25 mai 2016 et est applicable dans les pays de l'Union européenne depuis le 25 mai 2018.

Le RGPD a pour objectif de protéger les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.

Le RGPD s'applique donc aux traitements de données à caractère personnel, automatisés en tout ou partie, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans un fichier[1].

2. Les Services de Santé au Travail Interentreprises (ci-après « les SSTI ») ont pour objectif de faciliter la gestion et la prévention de la santé au travail pour leurs adhérents, à travers quatre missions :

- des actions en entreprise,
- du conseil,
- de la surveillance de l'état de santé,
- de la traçabilité et veille sanitaire.

Dans le cadre de leurs activités, les SSTI sont donc amenés à traiter des données à caractère personnel : ils sont par conséquent soumis aux dispositions du RGPD et doivent procéder à une mise en conformité.

Par ailleurs, il convient d'ores et déjà de préciser que compte tenu de leurs missions et leurs activités, les SSTI sont amenés à opérer des traitements de données à caractère personnel sensibles (données médicales).

La mise en conformité aux dispositions du RGPD par les SSTI présente donc un véritable enjeu.

3. La présente consultation juridique a donc pour objectifs :

- de présenter les dispositions du RGPD, d'une manière générale ;
- de les appliquer aux activités et missions des SSTI ;
- de répondre à différentes questions pratiques que se posent les SSTI dans le cadre de leur processus de mise en conformité.

A cet effet, la présente note a pour objet d'énoncer certaines des différentes étapes de mise en conformité qu'une entité doit respecter afin de se conformer aux exigences du RGPD.

[1] RGPD, article 2, §1

4. Il convient également de préciser que les étapes décrites ci-dessous sont des étapes qui peuvent être prises dans un ordre différent.

5. La présente note contient par ailleurs des éléments dits « pratiques » dans les différentes annexes. Ces documents sont proposés à titre d'exemple et peuvent bien entendus être améliorés ou modifiés.

6. Enfin, une foire aux questions (FAQ) a été réalisée afin de tenter de répondre aux différentes questions que les SSTI se posent dans le cadre de l'entrée en vigueur du RGPD.

La liste des questions a été établie sur la base de nos réflexions, et peut bien entendue être élargie en fonction des demandes des SSTI suite à la communication de la note.

La loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi Informatique et Libertés du 6 janvier 1978 afin d'exercer certaines des « marges de manœuvre nationales » autorisées par le RGPD.

Elle a également modifié certaines dispositions de la loi Informatique et Libertés pour les rapprocher de la lettre du RGPD.

Comme la CNIL l'avait relevé dans son avis sur le projet de loi, la bonne compréhension du cadre juridique suppose de lire de manière combinée le RGPD et la loi du 6 janvier 1978 ainsi « consolidée », puisque :

- certaines des dispositions de la loi du 6 janvier 1978, formellement inchangées, ne sont en réalité plus applicables dans le champ du RGPD, qui s'y substitue (par exemple : conditions de licéité des traitements, droit à l'information, etc.)

- la loi du 6 janvier 1978 n'est pas complète puisqu'elle ne mentionne pas tous les nouveaux droits ou obligations posés par le RGPD, pourtant également applicables (exemple : droit à la portabilité, obligation de réaliser des analyses d'impact, etc.).

- elle s'applique de manière différenciée dans les territoires d'outre-mer.

Une ordonnance de réécriture complète de la loi « Informatique et Libertés » est prévue, dans un délai de six mois, afin de répondre à ces trois enjeux de lisibilité du cadre juridique.

ETAPE N°1 : DETERMINER SA QUALITE DE RESPONSABLE DE TRAITEMENT OU DE SOUS-TRAITANT

La qualité de responsable de traitement ou de sous-traitant ne dépend pas de la nature de l'entité concernée par les traitements.

Il est possible qu'un même organisme soit responsable du traitement et sous-traitant d'un autre traitement, voire qu'il soit conjointement responsable avec d'autres de certains traitements.

Il est donc nécessaire de réaliser une analyse au cas par cas pour chacun des traitements auxquels l'organisme prend part.

De même, la qualité de responsable du traitement ou de sous-traitant ne dépend pas de la qualification des parties dans le contrat qui les lie.

La question qui se pose est donc de savoir dans quels cas les SSTI interviennent en qualité de responsable du traitement et en qualité de sous-traitants, compte tenu des différents traitements de données à caractère personnel effectués par les SSTI.

En effet, les SSTI effectuent des traitements de données à caractère personnel concernant leurs propres salariés, mais également concernant les salariés suivis.

Par ailleurs, les SSTI font appel à de nombreux prestataires informatiques qui vont les aider, de par la fourniture de différents services, à opérer ces traitements.

Les SSTI transmettent également de nombreuses informations concernant leurs salariés à des partenaires externes (sécurité sociale, organisme de formation…).

Les qualités de responsable du traitement ou de sous-traitant doivent donc s'apprécier en fonction des traitements effectués et des conditions de ces traitements.

I.1 La qualité de responsable du traitement

Le RGPD définit la notion de responsable du traitement de ma manière suivante[2] :

> *« […] «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre; […] »*

[2] RGPD, article 4, §7

Afin de déterminer si l'organisme agit en qualité de responsable du traitement, il est conseillé d'adopter une analyse en trois temps[3] :

- il convient d'abord de considérer la nature de la personne ou de l'entité qui pourrait être qualifiée de responsable du traitement : si une personne physique et une personne morale peuvent être désignées comme responsable du traitement, le G29[4] préconise qu'une telle qualification soit plutôt attribuée à une personne morale qu'à une personne physique en son sein, par exemple un salarié.

- il convient ensuite de déterminer si cette personne ou entité a un pouvoir décisionnel sur les finalités et les moyens du traitement : il convient de préciser que le terme « finalité » désigne l'objectif qui est poursuivi par le traitement ou qui guide les opérations de traitement : la détermination de la finalité du traitement est réservée uniquement au responsable du traitement.

  Les moyens du traitement peuvent être définis comme la façon d'atteindre un objectif : la détermination du type de données collectées, des personnes pouvant avoir accès à ces données, la durée de conservation de celles-ci, les personnes concernées par le traitement… Ces questions sont réservées au responsable du traitement également.

- il convient enfin de déterminer si ledit pouvoir décisionnel est exercé par une personne seule ou conjointement avec d'autres : il est possible que des entités soient coresponsables parce qu'elles participent ensemble à la détermination soit de l'ensemble des finalités et des moyens du traitement, soit uniquement des finalités ou uniquement des moyens ou d'une partie des finalités ou des moyens.

I.2 La qualité de sous-traitant

Il ressort des dispositions du RGPD que :

> *« […] «sous-traitant», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ; […][5] »*

> *« Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement[6]. »*

Aussi, pour agir en qualité de sous-traitant, il faut d'une part être une entité juridique distincte du responsable du traitement, et d'autre part traiter les données à caractère personnel pour le compte de ce dernier.

[3] G29, avis 1/2010, 16 février 2010
[4] Groupe de travail européen sur la protection des données à caractère personnel
[5] RGPD, article 4, §8
[6] RGPD, article 28, §3, a)

Il en ressort que le sous-traitant ne doit pas avoir de marge de manœuvre dans la détermination des finalités et des moyens essentiels du traitement : il n'a pas d'autonomie pour décider des objectifs poursuivis par le traitement ou des éléments essentiels (données traitées, personnes concernées, personnes ayant accès aux données…).

I.3 Le statut des SSTI

Il ressort de notre analyse qu'en synthèse, les SSTI opèrent des traitements de données concernant leurs salariés, les salariés suivis et leurs adhérents.

Il ressort de notre analyse que compte tenu des critères dégagés ci-avant :

- en ce qui concerne les données à caractère personnel de leurs salariés, ils agissent en qualité de responsable du traitement : les SSTI ont toute latitude pour déterminer seuls les finalités et les moyens des traitements des données à caractère personnel de leurs salariés.

- en ce qui concerne les données de leurs adhérents, ils agissent également en qualité de responsable du traitement, pour les mêmes raisons.

- en ce qui concerne les données qui sont transmis par les adhérents aux SSTI, ceux-ci agissent en qualité de sous-traitant.

- en ce qui concerne les données médicales des salariés suivis, et en ce qui concerne les données non-médicales collectées par le SSTI et autres que celles qui lui ont été fournies par les adhérents, les SSTI agissent en qualité de responsables du traitement : le SSTI va déterminer unilatéralement les moyens et les finalités des traitements opérés, sans les transmettre ensuite à l'adhérent.

- en ce qui concerne les prestataires informatiques des SSTI, lesdits agissent en qualité de sous-traitant des SSTI.

Point pratique : il ressort des éléments développés ci-avant que les SSTI sont à la fois responsables de traitements (dans la plus grande majorité des situations), mais également sous-traitants en ce qui concerne la relation avec leurs adhérents et notamment en ce qui concerne le traitement des données transmises par les adhérents.

Les SSTI interagissent par ailleurs avec des partenaires et des prestataires qui ont alors la qualité de sous-traitants à l'égard des SSTI.

Il convient donc de prendre en compte ces trois aspects dans le cadre de la mise en conformité des SSTI aux dispositions du RGPD.

Suite à la communication de la première note juridique, il apparait que certains SSTI défendent la thèse selon laquelle les SSTI auraient la seule qualité de responsable du traitement, même en ce qui concerne le traitement des données transmises par les adhérents sur les salariés suivis.

Cette thèse serait fondée sur les deux arguments suivants :

- les données des salariés suivis ne sont pas traitées que sur instruction des adhérents, mais dans le cadre de la mission de service de santé au travail ;

- les données seraient uniquement transférées pour que les SSTI remplissent leurs missions, sans que cela ne confère automatiquement aux SSTI la qualité de sous-traitant.

Bien entendu, cette analyse et ces arguments sont recevables, tout comme les conclusions qui en découlent.

Cependant, et malgré cette analyse contraire (encore une fois, uniquement en ce qui concerne le traitement des données des salariés suivis transmises par les adhérents des SSTI), nous maintenons notre position puisque selon nous, les données sont confiées pour l'exécution d'une mission de service de santé au travail, *« pour le compte des adhérents »* et *« sur instructions »* des adhérents.

En effet, selon nous, l'organisation de la santé au travail appartient aux employeurs[7] et ce sont ces derniers qui organisent les services de santé au travail[8].

Par conséquent, il existe soit des services de santé au travail « mutualisés », soit des services de santé au travail « autonomes » (lorsque les entreprises ont leur propre service de santé au travail interne).

Dans ce cadre, il ressort de notre analyse qu'un adhérent voit peser sur lui différentes obligations au titre de la médecine du travail à l'égard de ses salariés, et qu'en confiant cette mission à un SSTI et en lui transmettant les données de ses salariés pour l'exécution de cette mission, il place le SSTI en position de sous-traitant au sens du RGPD.

Bien entendu, nous ne pouvons affirmer que cette position est celle qui serait retenue par la CNIL si elle devait se positionner.

Il convient d'ailleurs de préciser que la CNIL, en cas de saisine de celle-ci sur la question, ne rendrait qu'un arbitrage qui aurait au moins le mérite de clarifier et de trancher la situation. Mais cet arbitrage serait tout aussi contestable en fonction de l'analyse de chacun.

A l'heure actuelle, et compte tenu des informations qui nous ont été communiquées, la CNIL n'a à ce jour pas été saisie officiellement d'une telle question, même si elle semble avoir été interrogée par différents SSTI.

[7] Article L.4621-1 du Code du travail
[8] Article L.4622-1 du Code du travail

En tout état de cause, il convient de préciser que (i) la question ne concerne qu'un point précis sur l'ensemble des traitements de données réalisés par les SSTI, qui restent dans la très grande majorité des cas responsables de traitements, et que (ii) cela n'a pas d'incidences fortes dans la mesure où le sous-traitant est soumis aux mêmes obligations de sécurité des données que le responsable de traitement.

ETAPE N°2 : DESIGNER UN DELEGUE A LA PROTECTION DES DONNEES

II.1 La désignation d'un DPO : obligatoire ou non ?

Le RGPD vient consacrer un nouvel acteur dédié à la conformité des traitements : le Délégué à la Protection des Données, également appelé dans la version anglaise le *Data Protection Officer* (ci-après le « DPO »).

Il ressort de l'analyse du RGPD que la désignation d'un DPO, par le responsable du traitement et/ou par le sous-traitant, n'est obligatoire que dans certains cas, à savoir :

> *« 1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:*
>
> *a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;*
>
> *b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou*
>
> *c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. […] »*[9]

En synthèse, la nomination d'un DPO est donc obligatoire dans différentes situations, et notamment lorsque l'activité de base du responsable du traitement ou du sous-traitant comprend un traitement à grande échelle constituant soit un suivi régulier et systématique des personnes concernées, soit concernant des données sensibles.

Ainsi, la désignation d'un DPO est obligatoire en cas de traitement à grande échelle de données sensibles.

Il convient de préciser que :

- la notion « d'activité de base » renvoie aux opérations essentielles effectuées par le responsable du traitement ou le sous-traitant ;
- la notion de « grande échelle » est très subjective et il conviendrait de retenir quatre facteurs, à savoir :

[9] RGPD, article 37, §1

- le nombre de personnes concernées ;
- le volume des données traitées ;
- la durée ou la permanence du traitement ;
- l'étendue géographique du traitement.

- les données de santé sont des données à caractère personnel dites « sensibles ».

Compte tenu de ces éléments, il ressort de notre analyse que les SSTI sont tenus de désigner un DPO, puisque les SSTI sont amenés, selon nous, à effectuer des traitements à grande échelle de données sensibles.

Par ailleurs, même si une analyse contraire est retenue, il ressort de notre analyse que même dans les cas où cela n'est pas obligatoire, la désignation d'un DPO par un SSTI témoignera de sa bonne volonté de placer la protection des données à caractère personnel au cœur de ses préoccupations.

II.2 La désignation du DPO : qui nommer ?

Le RGPD vient préciser que le DPO est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions qui lui sont confiées par le RGPD.[10]

Il ressort de différentes préconisations que la fonction de DPO doit rester ouverte à toute personne, quels que soient sa formation initiale et son parcours (notamment, recommandation de l'Association française des correspondants à la protection des données à caractère personnel (« l'AFCDP »)).

L'AFCDP recommande notamment que cette mission ne soit pas réservée aux seuls juristes.

Il est par ailleurs précisé par le RGPD que le niveau de connaissances spécialisées requis pour occuper la fonction de DPO doit être déterminé en fonction des opérations de traitement des données effectuées et de la protection exigée pour les données à caractère personnel traitées[11].

Ainsi, le niveau d'expertise requis, s'il n'est pas strictement défini, doit être adapté à la sensibilité, à la complexité et à la quantité des données traitées par un organisme.

Plus ces éléments sont élevés, plus le niveau d'expertise du DPO doit l'être également.

En synthèse, il nous est possible de préciser que le DPO doit :

- avoir une expertise dans les lois et pratiques nationales et européennes en matière de protection des données ;
- avoir une compréhension approfondie du RGPD ;
- connaitre le secteur d'activité de l'organisme responsable du traitement ;

[10] RGPD, article 37, §5
[11] RGPD, considérant 97

- avoir des connaissances techniques ;
- bénéficier d'une position au sein de l'organisme qui leur permet d'accomplir leur mission ;
- présenter des qualités personnelles intégrant un haut niveau d'intégrité et d'éthique personnelle.

Point pratique : il convient de préciser qu'il existe des formations (courtes ou longues) dédiées aux métiers de la conformité informatique, intégrant les dispositions du RGPD.

Il peut donc être utile de faire bénéficier le DPO d'une telle formation afin de le former et le sensibiliser à ses nouvelles fonctions.

Il convient enfin de préciser que le DPO peut être :

- interne (c'est alors un salarié de l'organisme) ;
- externe, au titre d'un contrat de services ;
- mutualisé (sous certaines conditions).

II.3 Le DPO : quelles fonctions et missions ?

Le RGPD vient organiser explicitement la fonction du DPO, en lui donnant tout d'abord une fonction générale, selon laquelle le DPO doit être associé par le responsable du traitement et le sous-traitant, dès le stade de la conception d'un produit ou d'un service et lors de la durée du traitement, à toutes les étapes de la mise en place d'un traitement de données à caractère personnel afin de pouvoir répondre aux questions relatives à la protection desdites données[12].

Cette démarche participe également à une approche *« Privacy by design »*[13].

En tant qu'interlocuteur privilégié, le DPO participe également aux différents groupes de travail consacrés aux activités de traitement ainsi qu'aux réunions et prises de décisions ayant des implications en matière de protection des données à caractère personnel.

Point pratique : l'avis du DPO doit toujours être pris en considération. En cas de désaccord, il est recommandé au DPO de rédiger un rapport dans lequel seront consignés les points de recommandations du DPO et les raisons pour lesquelles ces recommandations n'ont pas été suivies.

Par ailleurs, le RGPD vient préciser les missions du DPO[14] :

[12] RGPD, article 38
[13] Cf point V.
[14] RGPD, article 39

« a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;

b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;

c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35;

d) coopérer avec l'autorité de contrôle;

e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet. […] »

En synthèse, les missions du DPO sont donc :

- informer et conseiller ;
- contrôler la conformité ;
- former et sensibiliser coopérer avec l'autorité de contrôle ;
- être un point de contact.

Le responsable du traitement et le sous-traitant doivent aider le DPO à exercer ses missions, notamment en :

- lui fournissant les ressources nécessaires pour exercer ses missions, qu'elles soient humaines, matérielles, intellectuelles et/ou financières ;
- lui donnant l'accès aux données à caractère personnel et aux opérations de traitement ;
- lui permettant d'entretenir ses connaissances spécialisées, ce qui implique une obligation de formation[15].

Le DPO doit bénéficier d'une indépendance fonctionnelle, ce qui implique que le DPO ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions, et notamment sa façon de traiter un dossier : le DPO doit être libre d'adopter le point de vue qui lui semble pertinent dans l'analyse d'une question en matière de données à caractère personnel.

[15] RGPD, article 38, §2

Point pratique : compte tenu de l'élément précédent, il apparait que le DPO ne pourra être sanctionné ou licencié de manière directe ou indirecte pour l'exercice de ses missions de DPO, et par exemple en cas d'avis divergent.

Un risque de contentieux important en droit social peut être à prévoir si les responsables de traitement ne désignent pas des personnes compétentes et cherchent à les licencier.

Enfin, le DPO ne doit pas exercer de tâches donnant lieu à des conflits d'intérêts avec ses missions de DPO : il est donc déconseillé de nommer un membre de l'équipe dirigeante (Directeur juridique, Directeur des services d'information, Directeur des ressources humaines…) en qualité de DPO.

A titre de documents pratiques, un exemple de fiche de poste de DPO et de lettre de mission de DPO sont proposés en Annexes 4 et 5.

ETAPE N°3 : REALISER UN AUDIT DES TRAITEMENTS DES DONNEES A CARACTERE PERSONNEL

La réalisation du programme de mise en conformité passe nécessairement par la réalisation d'un audit.

Cet audit se réalise en plusieurs étapes :

III.1 Répertorier les données traitées et les traitements réalisés

Cette étape a pour objectif d'établir une sorte de cartographie des données et des traitements au sein de l'entité.

Pour cela, il convient tout d'abord d'identifier :

- des données traitées et de leur nature (sensibles ou non) ;
- de la nature des traitements ;
- des personnes concernées.

Cette étape doit être propre à chaque entité, les personnes concernées, les données traitées et les traitements réalisés pouvant différer d'une entité à une autre, et même d'un SSTI à un autre.

III.2 Lister les applications contenant des données à caractère personnel

Cette étape consiste à établir la liste des bases de données et des applications contenant des données à caractère personnel.

Cette liste doit contenir à la fois les applications et bases de données dites « propriétaires », c'est-à-dire les bases de données et les applications installées sur les serveurs de l'entité et sur lesquelles celle-ci a la parfaite maitrise, et les bases de données et les applications dites « progicielles », c'est-à-dire les logiciels mis à disposition en mode SaaS ou sur des serveurs par des éditeurs tiers.

Pour chacune des bases de données et des applications identifiées, il conviendra de lister :

- les données à caractère personnel traitées ;
- les durées de conservation mises en place ;
- la gestion des accès ;
- les mesures de sécurité associées.

III.3 Identifier les processus internes impliquant un traitement de données à caractère personnel

Il s'agit ici de déterminer les finalités pour lesquelles l'entité traite les données à caractère personnel et sur quelles bases ces traitements s'opèrent.

Il convient donc de s'entretenir avec l'ensemble des responsables de chaque direction métier, afin d'identifier avec eux :

- les processus internes impliquant les données personnelles ;
- les finalités pour lesquelles les données sont traitées ;
- les conditions de traitement de ces données, et notamment :
    - quelles sont les données collectées ;
    - comment sont-elles collectées ;
    - sont –elles transmises ou accessibles par des tiers, et sur quelle base (contrat…) ;

Cette phase d'audit permet d'établir un premier inventaire des traitements, qui permettra ensuite de compléter le registre des traitements (voir étape n°4) et de déterminer le niveau de maturité de l'organisme par rapport aux exigences du RGPD.

III.4 Déterminer son niveau de maturité

Le niveau de maturité du SSTI est basé sur les réponses obtenues lors de l'audit.

En pratique, il est possible de rédiger un document relatif à l'évaluation de la maturité du SSTI par rapport aux exigences du SSTI, en prenant en compte une échelle de maturité (par exemple de 1 à 4) (voir Annexe 6).

ETAPE N°4 : ETABLIR ET TENIR UN REGISTRE DES ACTIVITES DE TRAITEMENT

Le RGPD impose l'obligation pour les responsables des traitements et les sous-traitants de tenir un registre des activités de traitement effectuées sous leur responsabilité afin de démontrer qu'ils ont déployé les mesures de protection appropriées.

Ce registre doit impérativement être écrit et doit pouvoir être mis à disposition de la CNIL en cas de contrôle.

Les informations qui doivent figurer dans le registre des activités de traitement sont limitativement énumérées par le RGPD[16] :

> *« a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;*
>
> *b) les finalités du traitement;*
>
> *c) une description des catégories de personnes concernées et des catégories de données à caractère personnel; L 119/50 FR Journal officiel de l'Union européenne 4.5.2016*
>
> *d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;*
>
> *e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;*
>
> *f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;*
>
> *g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1. »*

Sur la base de cet inventaire, il conviendra alors de procéder à une pré-analyse d'impact sur les droits et libertés des personnes concernées, afin de déterminer les mesures techniques et organisationnelles de sécurité à mettre en œuvre pour garantir la licéité, l'intégrité, la confidentialité et la sécurité des traitements de l'entité.

[16] RGPD, article 30, §1

Il en résultera alors l'établissement d'un plan d'actions de mise en conformité, permettant de mettre en œuvre les mesures correctives nécessaires.

Point pratique : un exemple de registre des activités de traitement est présenté en Annexe 12.

ETAPE N°5 : ETABLIR SON PLAN D'ACTIONS

Le plan d'actions, ou programme de mise en conformité, regroupe les mécanismes internes permettant de démontrer le respect des règles relatives à la protection des données.

Ce plan d'actions ne doit pas se limiter à la simple énonciation des recommandations juridiques. Il doit être en réalité transversal, c'est-à-dire mobilisant l'ensemble des directions de l'organisme, détaillé, compréhensible et opérationnel.

V.1 les différentes étapes du plan d'actions

- Choix de l'équipe projet

Il ressort de notre analyse qu'en pratique l'équipe en charge de la mise en conformité aux dispositions du RGPD doit être composée, a minima :

- d'un juriste maitrisant la règlementation relative à la protection des données ;
- du responsable informatique ;
- de la personne en charge de la mise en conformité, cette mission revenant au DPO lorsque l'organisme en a désigné un.

Il convient de préciser qu'il peut par ailleurs être fait appel à des prestataires externes afin d'arrêter la manière de mener le projet et le calendrier en découlant.

- Audit des traitements et procédures internes et détermination du niveau de maturité

Comme il l'a été indiqué préalablement, cet audit a été réalisé ou doit être réalisé (voir ETAPE N°3).

- Détermination des actions à mettre en œuvre

A la suite de l'audit et de l'analyse de maturité, il convient de déterminer les actions à mettre en place afin d'assurer les garanties techniques et organisationnelles suffisantes pour répondre aux exigences du RGPD.

Le plan d'actions doit avoir pour objectif de pallier les risques identifiés par l'organisme lors de son audit.

V.2 Le contenu du plan d'actions

En synthèse, le plan d'actions doit contenir :

- la liste des recommandations juridiques du RGPD : cela concerne l'ensemble des exigences du RGPS (licéité du traitement, durée de conservation, sous-traitants, information et droits des personnes concernées, sécurité….)

- les livrables associés : il est préférable de traduire chaque action par un livrable associé. A titre d'exemple, concernant les SSTI, concernant la recommandation du RGPD relative à la mise en conformité des contrats, le livrable associé à cette action peut être l'avenant contractuel finalisé à diffuser à l'ensemble des adhérents du SSTI.

- le calendrier : il doit être fixé pour chaque action, prenant en compte (i) le niveau de priorité et (ii) le temps nécessaire à la réalisation de l'action.

- le coût de chaque action : il peut être envisagé de chiffrer le coût de chaque action, notamment en prenant en compte le ratio jour/homme sur la base du coût journalier de chaque personne affectée.

Il convient également d'indiquer le RACI *(Responsible – Accountable – Consulted – Informed)* associé à chaque action, étant précisé que :

- *Responsible* : celui ou ceux qui réalise(nt) l'action ;
- *Accountable* : celui ou ceux qui en est/sont responsable(s) ;
- *Consulted* : celui ou ceux qui participe(nt) ;
- *Informed* : celui ou ceux qui en est/sont informé(s).

Enfin, il convient de faire valider le plan d'actions par la Direction, si celle-ci n'est pas partie prenante à son établissement, afin de valider notamment le budget qui y sera alloué.

Point pratique : un exemple de plan d'actions est annexé à la présente consultation juridique (Annexe 12).

ETAPE N°6 : GARANTIR LE *PRIVACY BY DESIGN*

La notion de *privacy by design* (protection des données dès la conception) est consacrée par le RGPD[17] :

> *« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. »*

Il appartient donc au responsable du traitement de mettre en place un ensemble de mesures de sécurité en amont de la création de son produit, de son service et de la réalisation de ses traitements.

Le principe de *privacy by design* s'appuie sur sept piliers fondamentaux pour garantir l'effectivité de la protection de la vie privée dès la conception :

- le principe de proactivité : prévenir les risques d'atteinte à la vie privée avant qu'ils ne surviennent.

- le principe de protection par défaut : mettre en place un niveau de protection de la vie privée maximal, en veillant à ce que les données à caractère personnel soient systématiquement protégées au sein des systèmes informatiques et des pratiques des organismes.

- le principe de protection par construction : intégrer le principe dans les normes de conception des technologies, pratiques internes et infrastructures matérielles.

- le principe de conciliation des intérêts : il convient de prendre en compte tous les intérêts et objectifs légitimes.

- le principe de sécurité de bout en bout, durant tout le cycle de la vie de la donnée : il convient de garantir la sécurité pendant la période de conservation des données des personnes concernées, par des mesures essentielles à la protection de la vie privée en place du début à la fin.

[17] RGPD, article 25, §1

- le principe de visibilité et de transparence : fonctionnement du système conforme aux engagements établis.

- le principe de respect de la vie privée des utilisateurs : il convient de privilégier les intérêts des particuliers par des mesures strictes et implicites de protection de la vie privée axés sur l'utilisateur.

En pratique, la garantie du *privacy by design* peut se matérialiser en prenant les mesures suivantes[18] :

1. La restructuration de la gouvernance

En synthèse, il appartient au responsable de traitement de faire un état des lieux de son organisation en terme de gouvernance concernant la gestion des données à caractère personne, et de l'adapter si nécessaire aux exigences du RGPD, notamment par la nomination d'un DPO et de relais dans les différentes directions.

2. La minimisation de la collecte des données

Comme indiqué ci-avant, la minimisation de la collecte des données à caractère personnel est un des principes fondamentaux du RGPD.

En clair, il s'agit de collecter uniquement et exclusivement les données qui sont nécessaires à la finalité du traitement, et donc de minimiser autant que possible le nombre de données collectées.

Il appartient au responsable de traitement de procéder à un test de proportionnalité entre les données qu'il entend collecter et les finalités du traitement, tout en s'assurant qu'il n'existe pas d'autres moyens moins risqués pour la vie privée pour atteindre les mêmes finalités.

En effet, mois les données collectées sont nombreuses, plus les risques de violation de la vie privée sont limités.

Point pratique : lorsqu'on aborde la problématique de la minimisation de la collecte des données, il convient d'aborder la présence de zones de libres commentaires, présentes notamment dans les logiciels de gestion des services de santé au travail.

Ces zones représentent par nature un risque au regard des dispositions du RGPD, de part leur contenu qui peut ne pas être pertinent et conforme à la finalité du traitement.

En premier lieu, il convient tout d'abord de vérifier si cette zone de libre commentaire est pertinente ou non.

Dans l'hypothèse où elle serait pertinente, certaines recommandations ont été émises :

[18] Les développements suivants sont basés sur un rapport de l'agence européenne chargée de la sécurité des réseaux et de l'information (rapport ENISA, Privacy and data protection by design – from policy to engineering, janvier 2015)

- limitation de la taille de la zone ;
- ajout d'un texte de responsabilisation ;
- mise en place de mesures d'audit ;
- ajout de l'horodatage et de l'identité de l'auteur du commentaire.

En toute hypothèse, il ressort de notre analyse qu'une note d'information, de sensibilisation et de bonne conduite doit être transmise aux personnes utilisant de telles zones (que ce soit une note spécifique ou intervenant dans le cadre d'un document plus général).

3. La dissimulation des données

Il est conseillé, d'un point de vue technique, de dissimuler les données ainsi que leurs interdépendances.

Cette stratégie a pour but d'empêcher un éventuel pirate informatique de reconnaitre les liens entre les données.

Mais il convient que les données elles-mêmes ne soient pas visibles. Un des moyens techniques de dissimulation est la stéganographie.

4. La séparation des données

Cette stratégie consiste à séparer les données afin qu'elles ne soient pas toutes stockées au même endroit.

Il est ainsi possible de les stocker sur des bases de données différentes, ou à les séparer à nouveau au sein même des bases.

Cette technique présente deux avantages :

- la reconstitution du profil d'une personne est impossible ;
- il est possible d'établir une classification du risque sur les données en les séparant en fonction de leur niveau de risque et de criticité, et donc de prendre les mesures de sécurité adéquates en fonction du type de données (une adresse email ne présente par le même de niveau de criticité qu'une donnée médicale).

5. L'information des personnes

L'information des personnes est une obligation fondamentale prévue par le RGPD.

Cette transparence est d'ailleurs une des conditions de licéité du traitement.

Ce point est abordé à l'étape n°9 de la présente note juridique.

6. Le contrôle de la personne sur les données

Les personnes concernées doivent, en plus d'avoir été informées de l'ensemble de leurs droits et avoir obtenues l'ensemble des informations nécessaires, conserver une maitrise sur leurs données personnelles.

Cela passe par la garantie de plusieurs droit (droit d'accès, de rectification…) et par la mise en place, en pratique, de gestion desdits droits des personnes concernées.

Il est donc conseillé aux SSTI de mettre en place des procédures internes de gestion des droits des personnes concernées, et de les documenter.

7. La mise en œuvre d'une politique de confidentialité

Le responsable de traitement doit définir une politique de confidentialité décrivant :

- les données collectées ;
- la façon dont elles vont être utilisées ;
- les modalités d'exercice des différents droits des personnes concernées ;
- les mesures de protection mises en place.

Il appartient au responsable de traitement de faire respecter cette politique de confidentialité par l'ensemble de son personnel et de ses partenaires.

8. La preuve de la conformité

Il est toujours nécessaire de rappeler que le responsable de traitement doit être en mesure de prouver à tout moment la conformité de ses activités aux dispositions du RGPD.

Il appartient donc au responsable de traitement d'organiser une gestion documentaire de l'ensemble de ses démarches de mise en conformité et des livrables en découlant (documents contractuels, registres….).

Cela participera à la conservation des preuves nécessaires à démontrer le respect par le responsable de traitement des dispositions du RGPD.

ETAPE N°7 : CHOISIR SES SOUS-TRAITANTS ET ENCADRER LES RELATIONS CONTRACTUELLES

Le RGPD vient prévoir que le responsable du traitement doit uniquement faire appel à des sous-traitants qui fournissent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées au niveau de risque[19].

Cela implique pour les SSTI de choisir avec soin leurs prestataires, notamment informatiques, et de sécuriser juridiquement et opérationnellement les services fournis.

Les critères de sélection des sous-traitants pouvant être retenus sont les suivants :

- quelles sont les opérations de traitement confiées au prestataire ?
- quelle est la sécurité technique des services et donc des données ?
- quelle est le degré de maturité du prestataire concernant la protection des données à caractère personnel ?

Par ailleurs, il convient d'évaluer le niveau de risque du sous-traitant, afin de lui opposer les clauses contractuelles et les obligations adaptées au niveau des risques et ainsi assurer la sécurité, l'intégrité et la confidentialité des données personnelles traitées.

Pour mémoire, le RGPD impose au responsable du traitement de signer avec chacun de ses sous-traitants un contrat écrit contenant une série de clauses obligatoires[20] :

- l'objet ;
- la durée ;
- la nature et la finalité du traitement ;
- le type de données à caractère personnel ;
- les catégories de personnes concernées ;
- les droits et obligations du responsable du traitement.

Il convient également de gérer la chaine de sous-traitance dans son ensemble, c'est-à-dire de bien prendre en considération l'ensemble des sous-traitants de différents rangs.

Enfin, il convient de gérer la conformité des contrats à conclure ou déjà existants, en intégrant des dispositions spécifiques au RGPD, que ce soit dans le corps du contrat ou par voie d'avenant.

A ce titre, un exemple d'avenant contractuel est proposé en Annexe 7.

[19] RGPD, article 28, §1
[20] RGPD, article 28, §3

Point pratique : il apparait que les SSTI reçoivent régulièrement, de la part de leurs prestataires ou de leurs adhérents, des avenants contractuels à signer, spécifiquement liés aux dispositions du RGPD.

Il convient d'attacher une importance particulière aux termes de ces avenants, qui ont une véritable valeur contractuelle et qui doivent refléter la réalité des obligations mises à la charge de chacune des parties.

Il est donc conseillé aux SSTI de se munir de leurs propres documents contractuels et de les soumettre à leurs cocontractants en retour, les documents fournis par les cocontractants étant souvent trop génériques et non-adaptés à la relation.

Point pratique : il ressort de notre analyse que les contrats des prestataires informatiques (logiciels de gestion de la santé au travail, hébergeurs, prestataires d'infogérance…) prévoient dans la très grande majorité des cas une clause de limitation de la responsabilité des prestataires.

Ces clauses permettent aux prestataires informatiques de limiter leur responsabilité à un montant préalablement déterminé (par exemple, le montant annuel du contrat).

Si ces clauses ne présentent pas de difficulté en ce qui concerne la fourniture de la prestation en elle-même (sous réserve que le montant prévu soit accepté par l'ensemble des parties compte tenu du montant des préjudices pouvant être engendrés), il apparait qu'en termes de protection des données et de conformité aux exigences du RGPD, elles ne peuvent trouver à s'appliquer à notre sens.

En effet, le montant des préjudices en cas de violation de la sécurité des données, notamment en ce qui concerne les données de santé, ainsi que les amendes pouvant être infligées aux organismes en cas de non-conformité, sont bien supérieures (en théorie) aux montants prévus dans les clauses de limitation de responsabilité.

Il est donc impératif de prévoir une exclusion de la limitation de la responsabilité des prestataires en ce qui concerne la sécurité des données, afin que les SSTI puissent valablement se retourner contre les prestataires en cas d'inexécution contractuelle entrainant pour le SSTI un préjudice qu'il doit réparer.

Il convient donc de préciser que dans le cadre de la mise en conformité des contrats avec les prestataires informatiques, si un avenant spécifique au RGPD soit être signé, la clause de limitation de responsabilité doit être également renégociée afin de protéger au mieux les intérêts des SSTI.

Un exemple de clause est proposé en Annexe 8.

ETAPE N°8 : METTRE EN PLACE LES MESURES TECHNIQUES ET ORGANISATIONNELLES ADEQUATES

Le RGPD a introduit une obligation générale de sécurité qui se traduit par la mise en œuvre de mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Le devoir de sécurité comprend trois obligations distinctes :

- l'obligation de sécurisation, qui consiste à empêcher toute violation de données à caractère personnel, et à limiter l'accessibilité à ces données.

- l'obligation de notification, qui consiste à notifier à la CNIL toute violation de données à caractère personnel.

- l'obligation de communication qui consiste à communiquer toute violation de données à la personne concernée, si cela engendre un risque pour les droits et libertés.

En synthèse, le responsable du traitement et le sous-traitant doivent tout mettre en place, de façon proportionnée aux risques, afin d'éviter toute atteinte à la disponibilité, la confidentialité, l'intégrité et la traçabilité des données qu'ils traitent.

En effet, la sécurité du traitement est la contrepartie nécessaire de l'accès et de l'utilisation des données personnelles.

Le RGPD vient prévoir que[21] :

> *« 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:*
>
> *a) la pseudonymisation et le chiffrement des données à caractère personnel ;*
>
> *b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;*
>
> *c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;*

[21] RGPD, article 32

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre. »

Il convient donc de prendre des mesures techniques et organisationnelles adaptées et proportionnées.

Ces mesures dépendent :

- de l'état des connaissances ;
- des coûts de mise en œuvre ;
- de la nature, de la portée, du contexte et des finalités de traitement ;
- des risques, dont le degré de probabilité varie.

VIII.1 La mise en place de mesures techniques

Les mesures techniques de protection qui peuvent être mises en place sont les suivantes (liste non-exhaustive) :

- Sécuriser l'accès physique aux locaux

Il convient de mettre en place des dispositifs permettant de contrôler et limiter l'accès aux locaux (digicodes, badges), avec une sécurité renforcée en ce qui concerne la salle des serveurs et les salles où se trouvent des ordinateurs et dans lesquelles le public reçu n'a pas vocation à se rendre.

Il convient de noter que l'installation de dispositifs de vidéosurveillance doit obéir à des règles particulières d'utilisation (information des personnes, pas de salarié filmé sur son poste de travail, durée de conservation limitée…).

- Sécuriser les postes de travail

Il est nécessaire de mettre en place des mesures d'authentification des utilisateurs du système d'information : chaque utilisateur doit alors disposer d'un login et d'un mot de passe.

En ce qui concerne la complexité des mots de passe, la CNIL a élaboré un tableau de recommandations (voir Annexe 2).

Il convient de préciser que les mots de passe utilisés doivent être conformes aux recommandations de la CNIL, être secret, individuel et difficile à déchiffrer.

La CNIL recommande également un changement de mot de passe tous les trois mois (en s'assurant que le nouveau mot de passe soit différent des trois derniers) et qu'il soit attribué par l'administrateur du système mais immédiatement changé par l'utilisateur dès la première connexion.

La CNIL a également préconisé toute une série de mesures nécessaires à la sécurisation des postes de travail :

- verrouillage automatique des postes après maximum 10 minutes d'inactivité ;
- verrouillage du poste de travail dès que le salarié quitte son poste de travail ;
- installation d'un pare-feu logiciel ;
- limitation de l'ouverture des applications logicielles à celles strictement nécessaires ;
- mise à jour régulière des anti-virus et des logiciels ;
- limitation de la connexion à des supports mobiles (clés USB, disques durs externes…) au strict nécessaire ;
- utilisation des outils de prise en main à distance avec l'accord de l'utilisateur (éventuellement se munir de son propre outil ;
- non-utilisation de systèmes d'exploitation obsolètes.

Point pratique : l'ensemble de ces recommandations peut faire l'objet d'une fiche d'information à transmettre à l'ensemble des salariés du SSTI afin de les sensibiliser à la protection des données.

Cette fiche est ensuite à mettre dans la liasse documentaire liée à la mise en conformité au RGPD.

- Sécuriser le réseau local

Il est tout d'abords recommandé de mettre en place une journalisation et une traçabilité des actions sur les réseaux (création d'un historique des évènements réalisés).

Ensuite, la CNIL recommande la mise en place d'une politique d'habilitation afin d'assurer la confidentialité des données : il convient de pouvoir identifier les personnes qui ont accès aux fichiers. La politique d'habilitation doit définir les profils d'habilitation, mais elle doit également être mise à jour régulièrement afin de supprimer les permissions devenues obsolètes.

Enfin, il est recommandé de prévoir des dispositifs de sécurité (routeurs filtrants, pare-feu, sonde anti-intrusion…) et de veiller à la sécurisation des messageries électroniques et des connexions entre sites distants (protocoles IPsec, SSL/TLS, HTTPS).

- Sécuriser les données sauvegardées

La CNIL préconise que les données sauvegardées soient conservées de la manière suivante[22] :

- sauvegarde quotidienne des données modifiées par rapport à la précédente sauvegarde ;
- sauvegarde hebdomadaires complètes ;
- stockage des données dans un lieu sécurisé ;
- sécurisation des transferts de sauvegarde ;
- mise ne œuvre des mécanismes de chiffrement du canal de transmission des données dans le cas où la sauvegarde est automatisée sur le réseau ;
- stockage des supports de sauvegardes physiques (disques, cartouches…) dans des locaux différents de ceux où sont stockées les données traitées ;
- tests réguliers des sauvegardes ;
- contrôle de l'intégrité des données ;
- localisation géographique des sauvegardes.

- Organiser la pseudonymisation ou le chiffrement des données

La pseudonymisation est une mesure de sécurité technique qui consiste à remplacer une donnée à caractère personnel par un pseudonyme.

Aux termes du RGPD, la pseudonymisation est *« le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.[23] »*

La pseudonymisation est donc un traitement qui consiste à dissimuler dans une donnée les éléments relatifs à l'identité sans pour autant les faire disparaitre.

Elle suppose donc la réunion de deux conditions :

- une conservation séparée des éléments de ré-identification ;
- la mise en place de mesures techniques et organisationnelles tendant à empêcher la ré-identification.

[22] CNIL, Guide « Gestion des risques vie privée – Partie II : Catalogue de mesures », 2012
[23] RGPD, Article 4) 5)

Il convient de préciser que la pseudonymisation n'est pas l'anonymisation, qui vise quant à elle à supprimer tout lien direct ou indirect entre des données et une personne physique identifiée ou susceptible de l'être.

Le RGPD impose que les mesures prises soient adaptées aux données traitées.

Or, on peut distinguer trois techniques de pseudonymisation :

- la table de correspondance secrète : cela consiste à remplacer les identités par des pseudonymes, une table de concordance (pseudonyme / identité) étant établie en parallèle. La table de concordance doit alors être conservée avec un niveau de sécurité élevé. Cette technique présente un niveau de sécurité dit faible.

- le système cryptographique à clé secrète : cette technique permet de chiffrer et déchiffrer une donnée avec la même clé. La ré-identification se fait donc seulement par le seul détenteur de la clé, qui doit là encore être conservée avec un contrôle d'accès performant. Cette technique présente un niveau de sécurité intermédiaire.

- le hachage : une fonction de hachage calcule l'empreinte d'une donnée qui lui est passée. Cette empreinte est alors un identifiant unique de la donnée générée à un moment précis. Cette technique présente un niveau de sécurité élevé.

Pour mémoire, l'objectif est de réduire les risques de mise en corrélation d'un ensemble de données avec l'identité originale d'une personne physique.

Les mesures prises doivent là encore être adaptées aux types de données traitées.

Dans son dernier rapport d'activité, la CNIL préconise le chiffrement (deux dernières techniques susvisées) afin d'assurer la confidentialité des données à caractère personnel, notamment sensibles[24].

Les SSTI procédant aux traitements de données sensibles, ils sont invités à procéder à une pseudonymisation par chiffrement desdites données, lorsque cela est possible.

Il convient pour cela de se rapprocher de leurs différents prestataires informatiques.

Cependant, là encore, le RGPD fait peser sur les SSTI une obligation générale de moyens. Aussi, si un SSTI ne devait pas procéder à la pseudonymisation des données, notamment par chiffrement, il devra démontrer qu'il a tout mis en œuvre par ailleurs, au niveau organisationnel et technique, pour assurer la sécurité et la confidentialité des données, et ainsi préserver la vie privée des personnes concernées, que ce soit son personnel ou les salariés suivis.

VIII.2 La mise en place de mesures organisationnelles

[24] CNIL, 37ème rapport d'activité 2016

Le RGPD vient prévoir que les organismes doivent instaurer en leur sein une gouvernance de la donnée efficace et pertinente.

Les mesures organisationnelles qui pourraient ainsi être mises en place sont les suivantes, cette liste n'étant pas exhaustive :

- Elaboration d'un référentiel sécurité complet

Ce document a pour objet de lister toutes les mesures de sécurité prises au sein de l'entité concernée.

Il constitue à ce titre l'une des bonnes pratiques exigées par le RGPD, et notamment son article 32.

Il convient à ce titre de rappeler que la mise en conformité aux dispositions du RGPD passe par la preuve de cette mise en conformité, et inévitablement par l'élaboration de documents retraçant les constats effectués et les mesures prises pour pallier les éventuelles carences ou maintenir la conformité constatée.

Il convient donc de ne pas hésiter à établir une documentation complète et à la faire évoluer dans le temps.

Le référentiel sécurité fait partie de ces documents « inévitables ».

Il présente donc un intérêt légal, mais également (i) un intérêt commercial, dans la mesure où les partenaires ou clients (en l'espèce, s'agissant des SSTI, les adhérents, les salariés suivis et les collaborateurs) vont constater une maturité en matière de protection des données à caractère personnel, et (ii) un intérêt économique, dans la mesure où l'élaboration d'un référentiel sécurité performant, et le respect de celui-ci, permet d'éviter les cas de violation de données à caractère personnel dus à des failles de sécurité, et ainsi prévenir des éventuelles indemnisations ou amendes qui pourraient être coûteuses.

Point pratique : il n'est pas possible d'établir un référentiel de sécurité standard pour l'ensemble des SSTI, chacun d'entre eux devant établir ledit référentiel en fonction de son infrastructure informatique et de ses prestataires.

Les SSTI sont donc invités à interroger leurs prestataires informatiques, et notamment leurs hébergeurs, afin de solliciter leur propre référentiel de sécurité, qui s'intégrera forcément dans le référentiel sécurité du SSTI.

Enfin, à titre d'exemple, le référentiel sécurité peut comprendre :

- la politique générale de sécurité des systèmes d'information (PGSSI) ;
- la politique de durée de conservation et d'archivage des données ;

- le plan de continuité d'activité, en cas de sinistre ;
- la politique de gestion des incidents.

- La tenue d'un registre des failles de sécurité

Le RGPD vient préciser que *« en cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard ».*

Ainsi, tout responsable de traitement doit notifier à la CNIL, au plus tard dans les 72 heures, les failles de sécurité impliquant une violation des droites des personnes concernées, sauf si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés de celles-ci.

Il convient d'entendre par *« violation de données à caractère personnel »* une violation de sécurité entrainant de manière accidentelle ou illicite, la destruction, la perte l'altération, la divulgation non autorisée ou l'accès non-autorisé aux données à caractère personnel traitées (atteinte à l'intégrité, la disponibilité, la confidentialité ou la traçabilité des données traitées).

Le responsable de traitement doit également avertir individuellement les personnes concernées par la faille de sécurité.

Point pratique : il peut donc être utile de se munir d'une procédure d'avertissement des personnes concernées en cas de faille de sécurité constatée.

En parallèle, le responsable du traitement doit tenir un registre des failles de sécurité où sont recensés :

- la date des incidents ;
- le type d'atteinte ;
- l'importance de l'atteinte ;
- les mesures prises pour y remédier ;
- les mesures à prendre pour que l'atteinte ne se renouvèle pas.

Un modèle de registre des violations des données à caractère personnel est disponible en Annexe 9, et le formulaire de notification de violation fourni par la CNIL est disponible en Annexe 10.

Point pratique : Il apparait que le sous-traitant (au sens du RGPD) voit peser sur lui les mêmes obligations que le responsable de traitements, concernant notamment la signification des violations de données au responsable de traitement *(« dans les meilleurs délais »)* et la tenue d'un registre des failles de sécurité.

Par conséquent, les contrats avec les sous-traitants doivent venir prévoir ces obligations et être aménagés en fonction des impératifs de chacun.

- Gestion de la sécurité auprès des sous-traitants et des prestataires tiers

Il convient de préciser que d'une manière générale, en cas de violation de données à caractère personnel, le responsable de traitement sera responsable de l'ensemble des traitements qu'il aura mis en œuvre, que cette violation survienne de son propre fait ou de celui de l'un de ses sous-traitants.

Il sera bien entendu possible pour le responsable de traitement de se retourner ensuite contre le sous-traitant fautif (action récursoire), encore faut-il que les contrats liant le responsable de traitement (les SSTI) à ses sous-traitants (prestataires informatiques) lui permettent une telle action, d'où l'importance de la négociation et de la rédaction des contrats.

Ce point mérite donc une attention toute particulière.

Par ailleurs, les standards de sécurité du SSTI doivent soit être imposés aux prestataires, soit élaborés en partenariat avec eux.

Il convient donc de gérer ce point à la fois sur le plan technique, et sur le plan contractuel.

A cet égard, les contrats avec les sous-traitants doivent notamment prévoir que le sous-traitant :

- aide le responsable de traitement à satisfaire aux droits des personnes concernées ;
- aide le responsable de traitement à s'assurer de la sécurité des données ;
- supprime ou restitue les données à la fin du contrat ;
- s'engage à apporter toutes les preuves nécessaires au respect de ses obligations.

- La sensibilisation et formation du personnel

Il ressort des termes de cette note que la mise en conformité passe notamment par l'établissement de différents documents : référentiel de sécurité, procédures à respecter, registres, plan de continuité d'activité…

Cependant, le plus grand risque en matière de sécurité réside dans le facteur humain : c'est souvent lorsque les processus n'ont pas été respectés que la faille de sécurité se réalise (non-verrouillage des postes de travail, ouverture pièce jointe suspecte, clé USB égarée…).

Aussi, il est prépondérant de sensibiliser et de former les collaborateurs sur les mesures de sécurité à respecter, et effectuer des rappels très fréquemment.

Afin de limiter au maximum les risques de violation de données personnelles, les collaborateurs doivent être sensibilisés et formés aux bonnes pratiques, en complément des documents à valeur contraignante (charte informatique, processus…) qui leur sont communiqués.

La formation (notamment par des prestataires externes) des collaborateurs démontre un certain niveau de maturité et participe à démontrer la mise en conformité de l'organisme.

VIII.3 La réalisation d'analyses d'impact

L'analyse d'impact sur la protection des données est une nouveauté instituée par le RGPD[25].

- Qu'est-ce qu'une analyse d'impact ?

Le RGPD ne donne pas de définition formelle de la notion d'analyse d'impact.

L'analyse d'impact doit être vue comme un outil qui permet de vérifier et de démontrer la conformité d'un traitement de données à caractère personnel au principe de *privacy by design* (voir étape n°5).

En principe, l'analyse doit être réalisée avant la mise en place du traitement. En pratique, il convient d'en réaliser une, lorsque cela est nécessaire, dans le cadre du processus de mise en conformité.

En pratique, c'est un dossier documenté pour les traitements particulièrement sensibles qu'il convient d'établir.

- Quand l'analyse d'impact est-elle nécessaire ?

Il ressort des dispositions du RGPD que tous les traitements de données ne sont pas visées par la nécessité de réaliser une analyse d'impact :

> *« Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires. »*

[25] RGPD, article 35

Ainsi, le responsable de traitement est tenu de réaliser une analyse d'impact lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Devant cette injonction relativement vague, le G29 s'est attaché à préciser certains critères qui lorsqu'ils sont remplis par le traitement visé engendre la nécessité de réaliser une analyse d'impact :

- opérations d'évaluation des aspects personnels, de notation, de profilage et d'analyse prédictive ;
- prise de décision ayant des effets juridiques (établissement d'un contrat B to C par exemple) ;
- surveillance systématique ;
- données sensibles ;
- traitement à grande échelle ;
- données issues de deux traitements aux finalités différentes (séries de données assemblées et combinées) ;
- données concernant les personnes vulnérables ;
- recours à une nouvelle technologie ;
- privant d'un droit ou d'un service ;
- transfert des données en-dehors de l'UE.

Plus le traitement répond à un nombre de critères, plus il est probable qu'une analyse d'impact soit nécessaire.

Il ressort de notre analyse qu'à compter de la réunion de deux critères, l'analyse d'impact est nécessaire.

Or, à notre sens, les SSTI traitent des données sensibles (premier critère) à grande échelle (deuxième critère).

Une analyse d'impact semble donc nécessaire sur ce point-là (traitement des données de santé des salariés suivis), étant précisé que d'autres analyses d'impact peuvent être nécessaires selon les traitements effectués par les SSTI.

Il convient enfin de préciser que la CNIL est tenue d'établir une liste des opérations de traitement nécessitant une analyse d'impact.

- Que doit contenir l'analyse d'impact ?

Le RGPD vient préciser que l'analyse d'impact doit contenir *a minima* :

- une description des opérations de traitement et de ses finalités : une description générale du traitement, de ses finalités et de ses enjeux, ainsi que l'identification du responsable de traitement et des éventuels sous-traitants doivent être réalisées.

Par ailleurs, une description détaillée déterminant le périmètre du traitement, la nature des données concernées, leurs destinataires, la durée de conservation doit également être réalisée.

- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités : il convient là d'identifier les raisons pour lesquelles les données sont collectées, afin de répondre notamment au principe de minimisation de la collecte.

- une évaluation des risques pour les droits et libertés des personnes concernées : l'objectif est d'obtenir une bonne vision des causes et conséquences des risques. Il convient de mettre en avant les sources de risques (source humaine ou non humaine, interne ou externe, délibérée ou accidentelle), les évènements redoutés (l'accès illégitime aux données, la modification non-désirée des données et la perte de données), les menaces et les risques en découlant (avec une évaluation de la gravité et de la vraisemblance de chaque risque).

- la description des mesures envisagées pour faire face aux risques identifiés : les mesures peuvent être de différents ordres : juridiques, organisationnelles, techniques…

➢ Qui doit participer à l'analyse d'impact ?

Lorsque le responsable de traitement doit réaliser une analyse d'impact, il doit demander son avis au DPO[26], respecter les codes de conduite[27], et le cas échéant demander l'avis des personnes concernées ou de leurs représentants[28].

➢ Que faire quand l'analyse d'impact est terminée ?

Une fois le contenu de l'analyse d'impact élaboré, le responsable de traitement doit le valider, c'est-à-dire prendre la décision que les mesures envisagées sont suffisantes et que les risques résiduels peuvent être pris.

En présence de risques résiduels élevés, le responsable de traitement est tenu de consulter la CNIL.

Il convient enfin de noter que l'analyse d'impact n'a pas à être transmise aux personnes concernées.

Point pratique : afin d'accompagner les organismes dans leur mise en conformité et dans la réalisation des analyses d'impact, la CNIL a développé et mis gratuitement en ligne un logiciel spécifique : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

[26] RGPD, article 35 §2
[27] RGPD, article 35 § 8
[28] RGPD, article 35 § 9

ETAPE N°9 : GERER LES DROITS DES PERSONNES CONCERNEES

IX. 1 La licéité du traitement et le consentement

Il ressort des dispositions du RGPD que les données personnelles doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée.

La licéité du traitement est donc un élément prépondérant du respect des dispositions du RGPD, qui vient préciser que[29] :

> *« 1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:*
>
> *a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;*
>
> *b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;*
>
> *c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;*
>
> *d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;*
>
> *e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;*
>
> *f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.*
>
> *Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions. […] »*

Cet article introduit la notion de consentement des personnes concernées, notion fondamentale dans le cadre du RGPD.

Par ailleurs, en ce qui concerne les données à caractère personnel sensibles, et donc les données de santé, le RGPD vient indiquer que[30] :

[29] RGPD, article 6

« 1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie:

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée;

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée;

c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;

d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées;

e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée;

f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle;

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un 'État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée;

[30] RGPD, article 9

h) le traitement est nécessaire aux fins de la médecine préventive ou 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 sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3;

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel; L 119/38 FR Journal officiel de l'Union européenne 4.5.2016

j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée. […] »

En synthèse, cela signifie que par principe le traitement de données sensibles est interdit, sauf pour les exceptions listées précédemment, et notamment en ce qui concerne la médecine préventive et la médecine du travail.

Il convient de préciser que ces principes et exceptions ont été confirmés par le législateur français dans le cadre de la loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, qui a modifié la loi Informatique et Libertés afin d'exercer certaines des « marges de manœuvre nationales » autorisées par le RGPD (article 8).

En ce qui concerne les SSTI, il apparait que ceux-ci sont amenés à traiter, pour leurs salariés et les salariés suivis, deux types de données :

- des données à caractère personnel « simple » (non-sensible) : concernant cette catégorie de données, il convient de se référer à l'article 6 du RGPD, et ainsi se poser la question de savoir si les personnes concernées (adhérents, salariés du SSTI, salariés suivis) doivent donner leur consentement ou non concernant le traitement de leurs données.

  Il ressort de notre analyse que le consentement n'est pas nécessaire pour le traitement des données des personnes concernées précitées, dans la mesure où ce traitement relève de l'exécution d'un contrat (contrat de travail pour les salariés des SSTI, contrat d'adhésion pour les adhérents et contrat de travail pour les salariés suivis (ainsi qu'exécution d'une obligation légale)), sous réserve de respecter l'ensemble du cycle de licéité tel que défini ci-après.

- des données à caractère personnel sensibles : concernant cette catégorie de données personnelles, il convient de rappeler que leur traitement est interdit sauf lorsque « *le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail* ».

  Par conséquent, en ce qui concerne les salariés suivis, il ressort de notre analyse que l'obtention de leur consentement n'est pas nécessaire compte tenu de la finalité des traitements, à savoir la médecine préventive et du travail.

  Cependant, en ce qui concerne les salariés des SSTI, ces données de santé (ou toute autre données sensibles) ne peuvent être collectées sans le consentement du salarié, puisque les SSTI n'exercent aucune mission de médecine préventive ou du travail à l'égard de leurs propres salariés.

Point pratique : il convient de préciser que ces analyses relèvent de notre interprétation des textes, qui prévoient d'une part le consentement (1, a) de l'article 6 et 2, a) de l'article 9 du RGPD) pour ensuite prévoir une série d'exceptions audit consentement.

Nous en déduisons donc les exceptions au consentement comme indiqué ci-avant.

Cependant, cela reste sous réserve d'éventuelles interprétations contraires, notamment par la CNIL et par les tribunaux.

Nous pouvons donc vous conseiller, en cas d'interprétation contraire, d'obtenir le consentement de chacune des personnes concernées afin de vous prémunir de tous recours qui serait fait par une personne concernée.

IX.2 Les principes de licéité des traitements

Outre le principe de licéité des traitements en tant que telle, et l'éventuelle obtention du consentement, il convient de respecter différents principes afin d'assurer la licéité des traitements, relatifs à :

- la finalité des traitements (elle doit être déterminée, légitime, explicite, respectée) ;
- la qualité des données (minimisation, exactitude et mise à jour) ;
- la durée de conservation des données ;
- l'information des personnes concernées ;
- l'exercice par les personnes concernées de leurs droits.

IX.3 Les droits des personnes concernées et leur information

Les droits des personnes concernées existaient déjà avant l'entrée en vigueur du RGPD. Mais celui-ci est venu en renforcer certains et en a introduit de nouveaux.

Les droits des personnes concernées sont désormais les suivants :

- **Le droit à l'information de la personne concernée[31] :**

Le principe de transparence[32] impose que toute information et communication relative au traitement de données à caractère personnel soit aisément accessible, facile à comprendre et formulée dans des termes clairs et simples.

L'information des personnes dont les données sont collectées se matérialise par la diffusion de mentions obligatoires d'information, dont le contenu est encadré par la loi informatique et libertés et par le RGPD.

La diffusion de ces mentions obligatoires d'information peut prendre la forme de mentions apposées sur le formulaire de collecte, sur le site internet du responsable de traitement ou dans les clauses figurant sur les contrats.

Le contenu de l'obligation d'information est le suivant :

- informations sur les acteurs : nom et coordonnées du responsable de traitement, des sous-traitants, du DPO et éventuellement les catégories de destinataires ;
- informations sur le traitement : finalités du traitement, durée de conservation, intérêts légitimes poursuivis ;
- informations sur les droits des personnes concernées : droit d'accès, d'opposition, rectification, portabilité…, faculté d'introduire une réclamation auprès de la CNIL
- informations sur les transferts en-dehors de l'UE.

Lorsque la collecte a lieu directement auprès de la personne concernée, ces informations doivent lui être transmises immédiatement.

Lorsqu'elle est réalisée auprès de tiers (indirecte), l'information doit se faire dans un délai raisonnable (maximum un mois) ou au moment de la première communication.

Il existe des exceptions à l'obligation d'information lorsque la collecte est réalisée indirectement[33] :

- la personne concernée dispose déjà des informations (la preuve pèse sur le responsable de traitement) ;
- la fourniture de ces informations se révèle impossible ou exige des efforts disproportionnés ;
- la législation prévoit la communication des informations ;
- les données doivent rester confidentielles (secret professionnel).

[31] RGPD, articles 13 et 14
[32] RGPD, article 12
[33] RGPD, article 14 § 5

Point pratique : il ressort du présent développement que les SSTI doivent se munir d'un document d'information concernant à la fois le traitement des données de leurs salariés, mais également de celles des salariés suivis.

- **Le droit d'accès de la personne concernée[34] :**

Toute personne concernée peut demander au responsable de traitement la confirmation que des données à caractère personnel la concernant sont ou non traitées, et lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi qu'à un certain nombre d'informations (finalités du traitement, catégories de données concernées, destinataire des données, existence d'un transfert hors UE, durée de conservation…)[35].

Bien entendu, les personnes concernées doivent être informées des modalités et conditions de leur droit d'accès au moment de la collecte des données.

Le délai de réponse de l'organisme (étant précisé que le sous-traitant doit venir aider le responsable de traitement) doit répondre à la personne concernée dans un délai d'un mois (prolongement de deux mois possible *« compte tenu de la complexité et du nombre de demandes »* et si la personne concernée en a été informée dans le délai initial de un mois).

La réponse est par ailleurs gratuite, mais l'organisme peut se réserver la possibilité de solliciter le paiement de frais raisonnables si la demande engendre des coûts administratifs et que la demande est manifestement infondée ou excessive.

A ce titre, il convient de préciser que le responsable de traitement n'est pas tenu de répondre aux demandes de droit d'accès des personnes concernées lorsque :

- la demande est manifestement abusive, notamment par leur nombre, leur caractère répété ou systématique ;
- si les données ne sont pas conservées.

La charge de la preuve incombe au responsable de traitement qui doit également informer la personne concernée des voies de recours dont elle dispose.

Point pratique : il ressort de notre analyse que compte tenu du domaine d'activité des SSTI, et du nombre croissant de demandes liées à la protection des données, ceux-ci seront très probablement confrontés à des demandes de la part de leurs salariés, mais surtout de la part des salariés suivis.

[34] RGPD, article 15
[35] RGPD, article 15

Il est donc recommandé de mettre en place un processus interne de traitement des demandes d'accès, favorisant la transmission des informations par voie électronique.

- **<u>Le droit d'opposition à un traitement de données personnelles</u>**[36]

Le RGPD accorde à la personne concernée un droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement de données à caractère personnel la concernant.

Cependant, ce droit n'est pas absolu et un motif légitime doit être avancé par la personne concernée souhaitant bénéficier de ce droit.

Dans cette hypothèse, le responsable de traitement ne devra plus traiter les données à caractère personnel, à moins de démontrer qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts, droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense des droits en justice.

A l'heure actuelle, nous n'avons encore recul sur la difficulté de démontrer et prouver l'existence de ces motifs légitimes et impérieux (simple formalité ou travail plus poussé). EN tout état de cause, elle pèsera en premier lieu sur le responsable de traitement.

le droit d'opposition doit être explicitement porté à l'attention de la personne concernée au plus tard au moment de la première communication, de manière claire et séparément de toute autre information.

<u>Point pratique</u> : la question qui se pose concernant les SSTI est de savoir si un salarié suivi peut s'opposer au traitement de ses données dans le cadre de sa relation avec le SSTI.

Il ressort de notre analyse que le RGPD est venu restreindre le droit d'opposition des personnes concernées à certains domaines, et selon notre analyse, exclut du périmètre du droit d'opposition les cas de traitement suivants : le consentement de la personne concernée, <u>l'exécution d'un contrat avec la personne concernée, le respect d'une obligation légale</u> et la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne.

Aussi, il ressort de notre analyse qu'un cas de demande d'opposition d'un salarié suivi, et sous réserve que les données collectées soient strictement nécessaires aux finalités du traitement (médecine du travail), les salariés suivis ne peuvent exercer de droit d'opposition au traitement.

Cette analyse devra être précisée par la pratique mais il semble que le domaine de la médecine du travail et la nature des données transmises, sous réserve que le principe de minimisation de la

[36] RGPD, article 21

collecte soit respecté, constitue un motif légitime et impérieux permettant de ne pas accéder aux demandes d'opposition dans ce cadre-là.

- **Le droit de rectification de la personne concernée**[37]

Toute personne concernée a le droit d'obtenir du responsable de traitement, dans les meilleurs délais, la rectification des données personnelles la concernant qui sont inexactes.

Par ailleurs, compte tenu des finalités du traitement, la personne concernée a en outre le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.

En pratique, le responsable de traitement dispose de deux mois pour répondre de manière satisfaisante à la demande de la personne concernée, sauf motifs légitimes et impérieux.

Là encore, il peut être conseillé de mettre en place un processus de gestion des demandes de rectification.

- **Le droit à l'effacement ou « droit à l'oubli » de la personne concernée**[38]

Toute personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère la concernant.

Le droit à l'effacement comprend le droit au déréférencement et à la suppression des données personnelles collectées.

Ce droit n'est pour autant pas général et ne s'applique que pour des motifs limitativement énumérés, à savoir :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ;
- la personne concernée retire son consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique de traitement ;
- la personne concernée s'oppose au traitement et il n'existe pas de motifs impérieux et légitimes pour le traitement ;
- les données à caractère personnel ont fait l'objet d'un traitement illicite ;
- les données à caractère personnel doivent être effacées pour respecter une obligation légale.

Par ailleurs, des dérogations au droit à l'effacement sont prévues dans la mesure où le traitement est nécessaire :

- à l'exercice du droit à la liberté d'expression et d'information;

[37] RGPD, article 16
[38] RGPD, article 17

- pour respecter une obligation légale qui requiert le traitement, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
- pour des motifs d'intérêt public dans le domaine de la santé publique,
- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques dans la mesure où le droit visé est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement;
- à la constatation, à l'exercice ou à la défense de droits en justice.

➢ **Le droit à la portabilité des données personnelles[39]**

Le droit à la portabilité confère à la personne concernée le droit de recevoir les données à caractère personnel la concernant qu'elle a fournies à un responsable de traitement, dans un format structuré et couramment utilisé lisible par machine.

La personne concernée a alors le droit de transmettre ces données à un autre responsable de traitement, sans que le responsable de traitement initial ne puisse y faire obstacle.

Cependant, le RGPD prévoit une application limitée :

- aux traitements automatisés (exclusion donc des traitements manuels) ;
- aux traitements auxquels la personne concernée a consenti ;
- aux traitements nécessaires à l'exécution d'un contrat.

En ce qui concerne les SSTI, et donc matière de médecine du travail, l'article L.4624-8 du Code du travail vient préciser que :

> *« Un dossier médical en santé au travail, constitué par le médecin du travail, 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, notamment celles formulées en application des articles L. 4624-3 et L. 4624-4. Ce dossier ne peut être communiqué qu'au médecin de son choix, à la demande de l'intéressé. En cas de risque pour la santé publique ou à sa demande, le médecin du travail le transmet au médecin inspecteur du travail. Ce dossier peut être communiqué à un autre médecin du travail dans la continuité de la prise en charge, sauf refus du travailleur. Le travailleur, ou en cas de décès de celui-ci toute personne autorisée par les articles L. 1110-4 et L. 1111-7 du code de la santé publique, peut demander la communication de ce dossier. »*

C'est donc en l'espèce le Code du travail qui va venir préciser les conditions de transmission du dossier médical du salarié suivi, dossier qui contient l'essentiel des données à caractère personnel, notamment sensibles, des salariés suivis.

[39] RGPD, article 20

Point pratique : la mise en œuvre du droit à la portabilité impose des exigences organisationnelles non négligeables. Il convient donc de procéder par étapes :

Etape n°1 : l'information des personnes concernées

Comme précisé ci-avant concernant l'ensemble des droits, cette information doit être claire et explicite, au moment où les données sont collectées. Il peut être utile d'expliquer dans le cadre de l'information la différence entre droit d'accès et droit à la portabilité.

Etape n°2 : analyse de la demande

Le SSTI peut être amené à répondre à une demande de portabilité, ou il peut être destinataire d'une demande de portabilité.

(i) Lorsque le SSTI fait l'objet d'une demande de portabilité

En premier lieu, et en amont, le SSTI doit se poser la question de savoir si ses outils permettent d'assurer la portabilité des données (cela participe du *privacy by design*).

Ensuite, il convient d'identifier la personne concernée (un processus d'authentification est recommandé), la base juridique des traitements, les données et les traitements concernés.

Une fois ces éléments identifiés, le SSTI peut ou non faire droit à la demande, selon si celle-ci est éligible au droit à la portabilité.

(ii) Lorsque le SSTI est destinataire de données à caractère personnel au titre de la portabilité

Dans cette hypothèse, il convient de vérifier en amont que les données reçues sont compatibles avec le système d'information existant et correspondent à l'activité du SSTI.

Etape n°3 : exécution de la demande

(i) Lorsque le SSTI fait l'objet d'une demande de portabilité

Comme indiqué ci-avant, le SSTI peut ou non faire droit à la demande de portabilité.

Dans l'affirmative, il convient de transférer les données tout en précisant que le SSTI ne sera pas responsable de la manière dont les données sont ensuite utilisées, et d'en informer la personne concernée afin de se constituer la preuve du transfert.

Une mise en relation préalable avec le destinataire est indispensable afin de sécuriser à la fois le transfert, et la responsabilité du SSTI.

Dans la négative, il convient d'informer et de justifier auprès de la personne concernée les motifs du refus.

Nota Bene : le transfert ne peut être payant[40].

(ii) Lorsque le SSTI est destinataire de données à caractère personnel au titre de la portabilité

Dans le cas où le transfert des données est techniquement possible, il convient de :

- réaliser techniquement et de manière sécurisée l'opération ;
- en informer la personne concernée une fois les données réceptionnées, notamment afin de lui faire connaitre ses droits et de régler avec elle l'ensemble des éléments contractuels si cela n'a pas été fait avant.

Par ailleurs, il convient de vérifier que les principes issus du RGPS, et notamment celui de la minimisation de la collecte, est bien respecté, le SSTI destinataire étant le nouveau responsable de traitement et donc le nouveau garant du respect des droits de la personne concernée et des obligations légales relatives à la protection des données à caractère personnel.

Dans l'hypothèse où la portabilité n'est techniquement pas possible, il convient d'en informer la personne concernée et de trouver une solution avec l'organisme exerçant la portabilité.

- **Le droit au non-profilage[41]**

Le RGPD définit le profilage comme *« toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».*

Sans interdire le profilage, le RGPD est venu renforcer le droit des citoyens en prévoyant des garanties pour les personnes concernées.

Cependant, il ressort de notre analyse que cela ne concerne pas les activités des SSTI et ce droit (assez complexe) ne sera pas abordé dans le cadre de la présente note.

Il pourra toutefois faire l'objet de précisions en cas de demandes spécifiques des SSTI.

- **Le droit à la limitation du traitement des données personnelles[42]**

[40] RGPD, article 12
[41] RGPD, article 22
[42] RGPD, articles 18 et 19

Le droit à la limitation signifie que la personne concernée a le droit d'obtenir du responsable de traitement qu'il limite le traitement, cette limitation étant définie comme étant *« le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur »*[43].

Là encore, le droit consacré par le RGPD ne semble pouvoir être mis en jeu que dans des hypothèses relativement marginales, à savoir :

- l'exactitude des données personnelles est contestée par la personne concernée ;
- le traitement est illicite mais la personne concernée s'oppose à l'effacement des données et exige à la place une limitation de leur utilisation ;
- le responsable de traitement n'a plus besoin des données aux fins du traitement mais les données sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
- la personne concernée s'est opposée au traitement.

Seule la conservation des données est alors autorisée, sans qu'aucun traitement ne puisse être effectué.

[43] RGPD, article 4 § 3

ETAPE N°10 : MAINTENIR SA CONFORMITE DANS LE TEMPS

La mise en conformité au RGPD doit intervenir concernant les traitements existants, mais également concernant les traitements à venir, ou lorsque les traitements sont modifiés.

Ainsi, il convient au responsable du traitement et au sous-traitant de maintenir leur conformité dans le temps, en fonction de l'évolution de leurs activités et des nouveaux traitements qui pourraient être effectués (ou supprimés).

A cet effet, il peut être conseillé de :

- réaliser des audits internes, afin d'évaluer sa conformité et le maintien de celle-ci dans le temps ;

- réaliser des audits des sous-traitants, afin de vérifier que ceux-ci respectent bien leurs obligations contractuelles (à ce titre, il peut être intéressant d'insérer une clause d'audit dans les contrats conclus avec les prestataires) ;

En tout état de cause, il appartient aux SSTI de documenter les mesures de mise en œuvre, afin d'élaborer une sorte de « référentiel de conformité », qui permettra de justifier, le cas échéant, des mesures de mise en conformité entreprises par le SSTI.

CONCLUSION

Comme il l'a été évoqué ci-avant, le RGPD vient faire peser sur les SSTI de nouvelles obligations et la prise en conscience d'éléments nouveaux.

La protection des données personnelles peut pourtant être vue comme un enjeu majeur des années à venir.

Or, les SSTI se placent au centre de cette protection compte tenu de la nature sensible des données qu'ils sont amenés à traiter, et ils ne peuvent passer outre cette mise en conformité.

Aussi, si ladite mise en conformité peut être vue comme une contrainte (ce qui est nécessairement le cas, par nature), elle peut aussi être une opportunité de :

- rassembler l'ensemble des services autour d'un même sujet, le processus de mise en conformité étant nécessairement transversal,
- réduire les risques inhérents au sujet de la protection des données, et donc les risques financiers, la violation de données médicales pouvant entrainer des conséquences financières importantes,
- réduire les coûts qui pourraient servir à réparer les violations de données ou un contrôle de la CNIL, les mesures réactives étant souvent plus coûteuses que les mesures préventives,
- renforcer l'image et la réputation des SSTI, et ainsi la confiance de leurs adhérents.