**ANNEXE 1 : FOIRE AUX QUESTIONS**

|  |  |
| --- | --- |
| **QUESTIONS** | **REPONSES** |
| **Le consentement du salarié suivi est-il nécessaire pour collecter et traiter ses données personnelles et de santé ?** | Il ressort de notre analyse que conformément aux dispositions des articles 6 et 9 du RGPD, le consentement des salariés des SSTI et des salariés suivis n’est pas nécessaire pour collecter les données, sous réserve que les données collectées soient strictement nécessaires soit à l’exécution du contrat de travail, soit aux prestations de médecine du travail, ou que la collecte relève d’une obligation légale.  Dans le cas où le SSTI souhaiterait collecter des données à caractère personnel qui sortiraient de ce champ d’application, il serait alors nécessaire de récolter le consentement de la personne concernée. |
| **Que faire quand je reçois un avenant spécifique aux dispositions du RGPD envoyé par un prestataire ?** | Il ressort de notre analyse que les prestataires, et notamment les prestataires informatiques (logiciels, infogérance…) ont la qualité de sous-traitants. A cet effet, il n’est pas rare que les prestataires, dans un souci de mise en conformité des contrats, envoient un avenant au contrat de prestations, spécifique aux dispositions du RGPD.  Dans cette hypothèse, il apparait souvent que l’avenant (qui est souvent générique) ne soit pas conforme à la réalité des données traitées et des traitements confiés au prestataire.  Il convient donc de bien en prendre connaissance, et dans l’hypothèse où celui-ci ne reflèterait pas la réalité de la relation contractuelle, ou serait trop restrictif quant aux obligations du sous-traitant, il sera nécessaire de ne pas le signer et (i) soit de le négocier pour une nouvelle rédaction, (ii) soit de proposer son propre avenant contractuel, en votre qualité de responsable du traitement. |
| **Que faire quand je reçois un avenant spécifique aux dispositions du RGPD envoyé par un adhérent ?** | Là encore, il se peut que l’avenant envoyé soit trop générique et ne reflète pas la réalité de la relation.  Il convient donc là encore de l’adapter à la réalité de votre relation concernant le traitement des données.  D’une manière générale, en ce qui concerne la relation avec les adhérents, et sauf cas particuliers, il ressort de notre analyse que les SSTI peuvent se doter d’un avenant standard à leur contrat d’adhésion, qu’ils peuvent diffuser à l’ensemble de leurs adhérents pour acceptation et signature. |
| **Que faire quand je reçois une demande de la part d’un salarié (suivi ou du SSTI) ou d’un adhérent, relative aux mesures mises en place par le SSTI concernant la mise en conformité au RGPD ?** | Si votre SSTI a déjà mis en place une procédure de mise en conformité, il convient de faire parvenir à la personne concernée ou à l’adhérent qui en fait la demande une liste des mesures entreprises et de l’informer de ses droits, si cela n’a pas déjà été fait.  Si le SSTI est en cours de mise en conformité, ou si le SSTI n’a pas encore initié son processus de mise en conformité\*, alors il convient d’en informer la personne concernée ou l’adhérent, tout en l’informant de ses droits (un courrier type peut être dressé en ce sens afin de répondre à l’ensemble des demandes).  Un exemple de courrier est proposé en Annexes 16 et 17.  \*Il convient de préciser qu’il ne faut pas indiquer à l’adhérent ou la personne concernée que le processus de mise en conformité n’a pas commencé, mais qu’il est en cours (même s’il est encore embryonnaire). |
| **Comment gérer les contrats de travail au regard du RGPD ?** | Il convient à notre sens de communiquer à l’ensemble des salariés du SSTI, contre décharge, une notice d’information relative à leurs obligations concernant les traitements des données personnelles. Un exemple de notice vous est proposé en Annexe 19 et de décharge en Annexe 19 bis. Par ailleurs, en ce qui concerne les droits des salariés au regard des traitements de leurs données à caractère personnel, une fiche d’information peut leur être remise (Annexes 14 et 14 bis). |
| **Quelle est la qualité du SSTI au regard des dispositions du RGPD ?** | Il ressort de notre analyse que les SSTI ont plusieurs qualités au regard des disposions du RGPD :  - ils sont à la fois responsables de traitement concernant les données de leurs salariés, concernant le traitement des données de santé des salariés suivis (ainsi que concernant le traitement de données à caractère personnel des salariés suivis non-transmises par les adhérents), et concernant les données des adhérents.  - et sous-traitant en ce qui concerne les données à caractère personnel transmises par les adhérents concernant les salariés suivis. |
| **Un salarié suivi ou un salarié du SSTI a-t-il la possibilité de s’opposer à la collecte et au traitement de ses données ?** | Un salarié suivi ou un salarié du SSTI ne peut s’opposer au traitement de ses données à caractère personnel que s’il justifie d’un motif légitime supérieur aux motifs légitimes que pourraient lui opposer le responsable du traitement, sauf si les données personnelles avaient été collectées sur le fondement du consentement de la personne concernée.  A l’heure actuelle, nous n’avons que peu de recul sur la notion de « motif légitime » et sur le mode de preuve de celui-ci. |
| **Dois-je faire des formalités auprès de la CNIL ?** | Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l’administration de soins ou de traitements, ou de la gestion de services de santé, ne sont plus soumis à formalité auprès de la CNIL. Ils doivent cependant être inscrits dans le registre des activités de traitement et faire l’objet d’une analyse d’impact. |
| **Existe-t-il une liste des données à caractère personnel que les SSTI sont habilités / autorisés à traiter dans le cadre de leurs activités ?** | Il n’est pas possible valablement d’établir une liste exhaustive et précise des données que les SSTI sont autorisés à collecter, pour la seule raison que cette question doit être traitée au cas par cas, en fonction des spécificités de chaque SSTI et de chaque situation qu’il peut être amené à rencontrer.  Cependant, le principe applicable à l’ensemble des SSTI est le principe de minimisation de la collecte et de limitation des finalités : les données collectées doivent être indispensables à la finalité du traitement pour lequel elles sont collectées.  A défaut, si la collecte n’est pas nécessaire et qu’elle est dite de « complaisance », alors les dispositions et les principes du RGPD ne sont pas respectées.  En synthèse, tous les types de données à caractère personnel peuvent être collectés par les SSTI, sous réserve :  - que le traitement soit licite (consentement ou non) ;  - que la personne concernée soit informée des finalités du traitement, de l’identité du responsable du traitement, de la base juridique du traitement et des éventuels destinataires des données ;  - les données collectées soient pertinentes, adéquates et limitées aux finalités du traitement pour lequel elles sont collectées (principe de minimisation).  Pour plus de renseignements, se reporter à l’Annexe 3. |
| **Dois-je modifier ma charte informatique ?** | En premier lieu, il est fortement conseillé à chaque SSTI de se doter d’une charte informatique.  Par ailleurs, les chartes informatiques doivent être auditées afin de déterminer leur conformité aux nouvelles dispositions du RGPD.  En cas de non-conformité, elles doivent alors être mises à jour.  Les mesures essentielles à mettre en place afin d’assurer la sécurité su système d’information relèvent de (i) la sensibilisation et la formation, (ii) la connaissance du système d’information, (iii) le contrôle des accès, (iv) la sécurisation des postes de travail, (v) la sécurisation du réseau et (vi) la gestion du nomadisme (pour les salariés en déplacement ou bénéficiant de moyens informatiques portables, salariés en télétravail).  L’audit, la mise à jour (et éventuellement la refonte) de la charte informatique relèvent de la mise en conformité au RGPD pour les SSTI.  Il convient de préciser que la sensibilisation des salariés des SSTI à la manipulation des données à caractère personnel peut être intégrée dans la charte informatique, mais doit faire l’objet, à notre sens, d’une note d’information et de sensibilisation indépendante et spécifique.  Un exemple de charte informatique est proposé en Annexe 13. |
| **Comment dois-je informer les personnes concernées (salariés du SSTI, salariés suivis) de leurs droits ?** | Il convient de leur faire parvenir, au moment de la collecte, ou après lorsque cela n’a pas été fait au moment de la collecte, une fiche d’information synthétisant leurs droits et les informations rendues obligatoires par le RGPD.  Ces informations doivent être transmises *« de manière concise, transparente, compréhensible et aisément accessible. »*  Deux exemples de fiche d’information (salariés et salariés suivis) sont proposés en Annexes 14 et 15.  **ATTENTION : lorsque la collecte est indirecte, ou lorsque la fiche d’information n’a pas pu être remise au moment de la collecte, il convient de répertorier les données déjà collectées (voir Annexes 14 bis et 15 bis).**  Afin de se constituer la preuve de la remise de ses fiches d’information, vous pouvez :  - concernant les salariés du SSTI : soit la faire signer par vos salariés ou la diffuser par email ;  - concernant les salariés suivis : soit leur faire signer à chaque visite, soit simplement leur remettre en mains propres : il sera alors plus dur de prouver que vous leur avez bien remis. Aussi, vous pouvez afficher cette fiche dans la salle d’attente, en laisser en libre disposition, la diffuser dans le cadre d’une information générale diffusée par email (newsletter…). **ATTENTION**: plus la fiche est diffusée, plus vous vous exposez à des demandes des salariés suivis concernant le traitement de leurs données, ce qui peut être fastidieux à traiter. Il convient donc d’agir selon le principe de proportionnalité. |
| **Le comité d’entreprise de mon SSTI est-il concerné par le RGPD ?** | Il ressort de notre analyse que si les comités d’entreprises bénéficiaient d’une dispense de déclaration par la CNIL (dispense n°10), le RGPD est venu « rebattre les cartes » (voir Annexe 18).  A notre sens, et en l’état actuel des choses, notre analyse est de dire que les comités d’entreprises doivent se mettre en conformité avec le RGPD en tenant notamment un registre des traitements, en respectant les principes du RGPD (minimisation, information des personnes concernées…).  Cependant, cela n’est pas aujourd’hui une certitude et il convient d’attendre de vois la position de la CNIL sur ce sujet. |
| **Dois-je déclarer le DPO à la CNIL ?** | Oui, le DPO doit être déclaré à la CNIL. Vous pouvez le déclarer en ligne à l’adresse suivante :  <https://designations.cnil.fr/dpo/designation/organisme.designant.delegue.action> |