4. ACTIONS MISES EN ŒUVRE AU SEIN DE SIST OUEST NORMANDIE

Afin de respecter les principes fondamentaux du RGPD énumérés au chapitre I, SIST Ouest Normandie met en œuvre les 7 actions suivantes :

1. Désignation d'un DPO (Art 37 à 39 du RGPD)

Le Service a nommé un DPO qui a pour mission de veiller au bon respect de la LIL et du RGPD.
Le DPO a un rôle de conseil, de recommandation et d'alerte s'il constate des manquements. Il est informé préalablement à la mise en œuvre des traitements et des projets de traitements de données.

2. Tenue d'un registre des activités de traitement (Art 30 du RGPD)

Registre comprenant : l'identité et les coordonnées du responsable de traitement, les finalités de traitement des données à caractère personnel, les destinataires des données, la durée de conservation des données à caractère personnel (si impossible, critères utilisés pour déterminer cette durée)

3. Information et respect des droits des personnes concernées (Art 12 à 23 du RGPD)

Le Service informe les personnes de l'objectif de la collecte de leurs données, de l'utilisation de celles-ci ainsi que des droits dont ils disposent : droit d'accès, de rectification, d'effacement, de limitation et d'opposition. Cette information est notamment effectuée par :

- La charte informatique interne (chapitre 6) ;
- Les CGU de l'espace personnalisé Adhérent (chapitre 6) ;
- Les CGU (chapitre 6) et les fonctionnalités « Autorisation et consentements » de l'espace salarié ;
- Les mentions RGPD du site internet SIST Ouest Normandie ;
- L'affichage en salle d'attente relatif aux dossiers médicaux en Santé au Travail (DMST) ;

Le Service dispose par ailleurs de modes opératoires relatifs au partage de données de santé en interne, au transfert de DMST et au recueil de consentements (téléconsultation et communication de données non anonymisées à des tiers).

4. Garantie de la sous-traitance du traitement de données (Art 28 du RGPD)

Focus Logiciel métier : le prestataire sélectionné par SIST Ouest Normandie est certifié ISO 27001 et ISO 27701 (sécurité des données).
L'hébergeur des données intégrées au logiciel métier est certifié hébergeur de données de santé (HDS).

5. Traitement des éventuelles violations de données (Art 33-34 du RGPD)

Le Service analyse les incidents détectés en identifiant si des données à caractère personnel sont impliquées. Si c'est avéré, l'incident est traité par la Direction des Systèmes d'Information en tant qu'une violation de données dans la mesure où les données sont détruites, altérées ou divulguées.

6. Sensibilisation des collaborateurs (Art. 39 du RGPD)

- Sensibilisation dès l'embauche de nouveau collaborateur via le parcours d'intégration
- Charte d'utilisation des technologies de l'information et de la communication (notamment son chapitre 6)

7. Traitement des questions et des réclamations utilisateurs

Les utilisateurs peuvent prendre contact avec le DPO pour toute question ou réclamation relative au traitement de leurs données à caractère personnel et à l'exercice de leurs droits : par voie postale à l'adresse du siège de SIST Ouest Normandie ou par mail à dpo@santetravail-on.fr