Analyse d'impact relative à la protection des données (AIPD)

Gestion des dossiers sociaux par le Service Social Départemental (SSD)

Avis de la DPD et des personnes concernées

Le traitement est nécessaire à l'exécution d'une mission d'intérêt public. Il doit être mis en œuvre avec les mesures de sécurité listées dans la présente et améliorées selon le plan d'action.

Vue d'ensemble

Quel est le traitement qui fait l'objet de l'étude ?

Logiciel métier du SSD (NOVA) :

- gestion des RDV et planning des CSS
- dossier administratif de l'usager
- dossiers sociaux : dossiers complétés au fur et à mesure de l'accompagnement de l'usager
- exploitation des données :
- traitements statistiques anonymisés via l'infocentre mis à disposition par l'éditeur ;
- export de données nominatives via des requêtes définies avec l'éditeur (ex : liste des usagers suivi par un professionnel) pour le suivi des usagers et le pilotage d'activité.

Quelles sont les responsabilités liées au traitement ?

Le traitement des données est assuré par le Département de la Seine-Saint-Denis en particulier, le Service Social Départemental (SSD) de la Direction de la Prévention et de l'Action sociale (DPAS).

L'hébergement des données est assuré par Wordline-Santeos.

Quels sont les référentiels applicables ?

Wordline est certifié hébergeur de données de santé (certification HDS 1.1 juin 2018) certificat daté de juin 2019.

Données, processus et supports

Quelles sont les données traitées ?

Les données recueillies concernent les usagers des CSS
- données administratives des usagers
- données socio-économiques*
- données concernant les difficultés sociales des usagers* (problématiques famille, financières, insertion sociale ou professionnelle, administratives, logement/hébergement, santé, problématique numérique)

*Ces données ne sont collectées qu'en fonction des besoins de l'accompagnement social.

Durée de conservation des données des usagers : 2 ans à partir du dernier contact

Les données concernent également les professionnels des centres :
- traces de navigation (traçabilité des accès) / consultation / modifications des dossiers usagers

Destinataires potentiels :
- professionnels du service social
- services internes du département (SSOLOG, SAG...)
- partenaires institutionnels (CAF, France Travail, Projets Insertion Emploi, missions locales, CNAV, CRAMIF, CCAS, préfecture, associations...)

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

Données saisies dans les circonscriptions de service social :

- Création de la fiche identité de l'usager à la 1ère rencontre avec l'usager
- pose de rendez-vous entre l'usager et un professionnel
- accompagnement social de l'usager

- ajout de données, de pièces nécessaires (édition ou intégration de courriers, comptes-rendus d'entretien, pièces justificatives...)

Pendant la durée de vie du dossier : hébergement des données chez l'éditeur.

- Après 2 années d'inactivité du dossier : aléatoirement 10% des dossiers sont versés numériquement aux archives départementales et suppression numérique du reste des dossiers par Santeos.

En principe, le dossier social de l'usager est unique et rattaché à une seule circonscription C'est pourquoi, dans certains cas, un dossier peut être récupéré par une autre CSS après détachement de la circonscription d'origine, ex : signalements/ déménagements

Des statistiques peuvent être effectuées avec les données anonymisées disponibles dans l'infocentre par le service central.

Quels sont les supports des données ?

- Logiciel NOVA
- Serveurs de l'hébergeur

Proportionnalité et nécessité

Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

La finalité du traitement est de faciliter la gestion de l'accueil des usagers en circonscription de service social et le suivi des dossiers créés pour l'accompagnement social.

Le traitement permet à tout professionnel de la circonscription de noter l'ensemble des actions et interventions qu'il réalise dans le dossier social d'une personne, de consulter ce dossier afin de répondre à l'usager sur l'état d'avancement des actions le concernant.

Outre la tenue du dossier social, les données recueillies et traitées sous forme statistiques permettent également de remplir la mission de « veille sociale » exprimée notamment dans l'article L116-1 du code de l'action sociale et des familles.

L'outil permet également d'organiser le pilotage de l'activité des circonscriptions.

Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?

Fondement légal du traitement des données personnelles :

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.

Le Conseil Départemental de Seine-Saint-Denis est une collectivité territoriale (article 72 de la Constitution).

La loi de modernisation de l'action publique territoriale et d'affirmation des métropoles (MAPTAM) du 27 janvier 2014 et la loi portant nouvelle organisation territoriale de la République (NOTRe) du 7 août 2015 désignent le département comme **"chef de file" en matière d'aide sociale, d'autonomie des personnes et de solidarité des territoires**.

Le code de l'Action Sociale et des Familles prévoient notamment que « *Le département définit et met en œuvre la politique d'action sociale, en tenant compte des compétences confiées par la loi à l'Etat, aux autres collectivités territoriales ainsi qu'aux organismes de sécurité sociale. Il coordonne les actions menées sur son territoire qui y concourent. Il organise la participation des personnes morales de droit public et privé mentionnées à l'article L. 116-1 à la définition des orientations en matière d'action sociale et à leur mise en œuvre. » (L121-1).*

Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

Seules les données d'identité indispensables à la création du dossier (nom – prénom – date de naissance- sexe) sont obligatoires dans le logiciel. Les autres informations, tant sur l'identité que sur la situation sociale, ne sont saisies que selon les besoins.

L'appréciation des difficultés est recueillie d'abord pour évaluer la situation sociale de la personne mais aussi, le cas échéant, en vue de la sollicitation d'un dispositif réglementaire particulier.
Conformément à l'éthique et à la déontologie du travail social, les données doivent être les plus factuelles et objectives possibles, et ne sont de toutes façons notées que si elles présentent un intérêt pour l'évaluation de la situation de l'usager et les actions en sa faveur.

Les données sont-elles exactes et tenues à jour ?

Les données transcrites sont exactes en fonction des informations transmises par l'usager et tenues à jour par les professionnels du service au gré des entretiens.

Quelle est la durée de conservation des données ?

Les données sont conservées durant la vie du dossier et deux ans après le dernier contact avec l'usager.

Mesures protectrices des droits

Comment les personnes concernées sont-elles informées à propos du traitement ?

Des affiches figurent dans les salles d'attente et à l'accueil des CSS comportant une mention sur le droit d'accès et rectification des données personnelles.

Les personnes sont informées oralement des finalités du traitement et de leurs droits lors de l'échange avec l'usager en vue de la création du dossier social.

Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Le traitement a pour fondement légal principal la mission d'intérêt public. Un consentement spécifique pour l'envoi d'un SMS automatique pourra être demandé.

Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit à la portabilité ?

Concernant le droit d'accès :

L'usager devra formuler une demande directement auprès de la Déléguée à la Protection des Données du Département de la Seine-Saint-Denis. Celle-ci sera formulée par mail ou par courrier.

Comment les personnes concernées peuvent-elles exercer leurs droit de rectification et droit à l'effacement (droit à l'oubli) ?

Les usagers ont la possibilité de faire rectifier leurs données : cette demande devra se faire directement auprès de la circonscription compétente pour son accompagnement.

Les professionnels disposant des habilitations (référents dans les centres ou administrateurs) procèdent aux rectifications.

Comment les personnes concernées peuvent-elles exercer leurs droit de limitation et droit d'opposition ?

L'usager peut demander aux professionnels de la circonscription en charge de son dossier à ce que ses données ne fassent plus l'objet d'un traitement durant un temps déterminé. La DPD devra en être informée.

Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Un marché public attribué à SANTEOS-WORDLINE a été signé dans lequel figure les obligations du sous-traitant.

En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Sans objet.

Mesures existantes ou prévues

Chiffrement

Le chiffrement est organisé par Santeos
Les données chiffrées sont :

- les données structurées de l'usager (fiche état civil)
- la clé de chiffrement de l'usager
- Les notes et observations de consultation sont chiffrées
- les commentaires des rendez-vous sont chiffrés

Le dossier médical (nommé dossier social dans NOVA pour le service social), les pièces jointes y compris sont chiffrés.

Contrôle des accès logiques

Définition des profils utilisateurs par corps professionnels avec droits respectifs.

Authentification : mot de passe/login

Dans NOVA, chaque action fait l'objet d'un contrôle d'accès. Même si une action n'est pas proposée à l'utilisateur si son profil ne lui permet pas de l'exécuter, un contrôle supplémentaire est effectué côté serveur avant de « servir » une fonctionnalité.

Contrôle d'intégrité

Certification HDS

Les règles de sécurité applicables à l'hébergement sont décrites dans le Plan Assurance Qualité (PAQ) ainsi que dans le paragraphe dédié à la présentation des Data Center de Seclin.

Journalisation

Toutes les actions de l'utilisateur lors d'une session sont tracées

Archivage

L'archivage des données médicales ou sociales de NOVA est assuré par le Département via l'archivage des sauvegardes des données de NOVA.

La politique de durée de rétention et de stockage des archives est laissée à la discrétion du Département.

Santeos recommande la production d'une archive avant l'exécution des traitements de destruction de dossiers.

Sécurisation des documents papier

Les documents papiers sauvegardés sont les dossiers des usagers.

Gestion des postes de travail

- Authentification AD
- Verrouillage automatique
- Ordinateur inaccessible au public
- Respect de la PSSI départementale

Sécurisation de l'exploitation

L'exploitation est déléguée à SANTEOS-WORDLINE dans le cadre du marché.

Sauvegarde des données

Sauvegardes journalières gérées par l'éditeur et le Département.

Cloisonnement

Cloisonnement des données par services et profils.

Traçabilité

Traçabilité et historique accessibles par les administrateurs de l'outil NOVA.

Contrat de sous-traitance

Existence d'un marché public :
Santeos : intégrateur de l'application
Wordline: hébergement

Sécurisation des canaux informatiques

Documentation éditeur conforme à la PSSI départementale.

Sécurité physique

Datacenter sécurisé avec normes à jour.

Lutte contre les logiciels malveillants

Installation d'un anti-virus sur tous les postes de travail

Protection des sites web

Certificat de sécurité à jour et conforme.

Organisation de la politique de protection de la vie privée

- Nomination d'un DPO
- Notes envoyées en 2018 sur la mise en conformité RGPD
- Conférences de sensibilisation vie privée
- Note du service social départemental
- Affiches de sensibilisation
- Nomination de relais RGPD au sein des services
- Processus de gestion des violations de données

Accès illégitime à des données

Impacts potentiels :

Atteinte à la vie privée.

Menaces :

- Usurpation d'identité
- Fuite de mot de passe
- Manquement dans la sécurité des postes de travail
- Accès physiques non surveillés
- Phishing/virus

Sources de risques :

- Source humaine interne malveillante,
- Source humaine interne accidentelle,
- Incident chez l'éditeur : incendie, défaillance technique, source humaine externe agissant de manière délibérée,
- Source humaine extérieure malveillante

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Chiffrement, Gestion des postes de travail, Contrôle des accès logiques, Journalisation, Archivage, Contrôle d'intégrité, Sécurisation des documents papier, Sécurisation de l'exploitation, Sauvegarde des données, Cloisonnement, Sécurité physique, Lutte contre les logiciels malveillants, Protection des sites web

Modification non désirée de données

Impacts :

Retard dans la prise en compte de la situation de la personne concernée

Menaces

- Usurpation d'identité
- Fuite de mot de passe
- Manquement dans la sécurité des postes de travail
- Accès physiques non surveillés
- Erreur
- Phishing/virus

Sources de risques

- Source humaine interne malveillante,
- Source humaine interne accidentelle,
- Source humaine extérieure malveillante

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Chiffrement, Archivage, Contrôle des accès logiques, Sécurisation des documents papier, Journalisation, Gestion des postes de travail, Traçabilité, Contrôle d'intégrité, Cloisonnement

Disparition de données

Impacts :

Perturbation temporaire de l'accompagnement de la personne concernée

Menaces :

- Mauvaise manipulation
- Shutdown
- Usurpation d'identité
- Fuite de mot de passe
- Manquement dans la sécurité des postes de travail
- Accès physiques non surveillés
- Phishing/virus

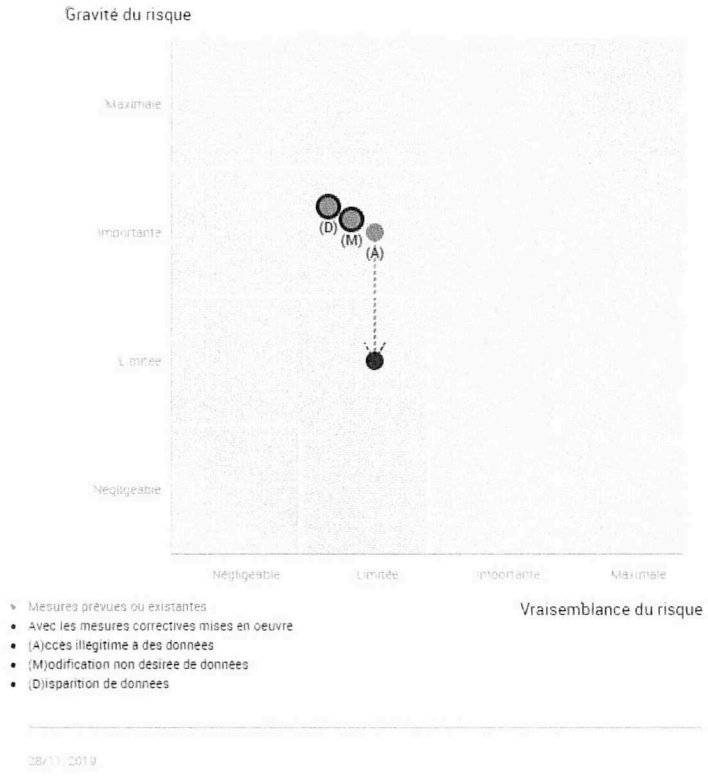
Quelles sources de risques pourraient-elles en être à l'origine ?

Source humaine interne malveillante, Source humaine interne accidentelle, Source humaine extérieure malveillante, Source naturelle (incendie, inondation...)

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Chiffrement, Contrôle des accès logiques, Archivage, Sauvegarde des données, Sécurisation de l'exploitation, Traçabilité, Sécurisation des canaux informatiques, Sécurité physique, Sécurisation des documents papier, Lutte contre les logiciels malveillants

Cartographie des risques



Nom et fonction (Qualité de Directeur ou chef de Service requise)	**Signature** (Précédé de la mention « **Lu et approuvé** »)
GERAADS Matthieu Directeur	Lu et approuvé Matthieu GERAADS Directeur de la Prévention et de l'Action Sociale