Registre Général de Protection des Données

AST BTP DE L'AIN

Coordonnées du responsable de l'organisme	***Président : Xavier RENAUD*** *33 rue Bourgmayer – 01000 Bourg en Bresse* *Tél : 04 74 23 58 30* *Mail : bourgenbresse@astbtp01.fr*
Nom et coordonnées du délégué à la protection des données	***Directrice : Marie-France CAILLAT*** *33 rue Bourgmayer – 01000 Bourg en Bresse* *Tél : 04 74 23 58 30* *Mail : mf.caillat@astbtp01.fr*

Activités	Désignation des activités
Activité 1	***Le suivi médico-professionnel des salariés***
Activité 2	***Les entreprises adhérentes***
Activité 3	***Les fournisseurs***
Activité 4	***La comptabilité générale***
Activité 5	***La paie***
Activité 6	***Les ressources humaines***
Activité 7	***L'accès aux locaux***

Activité 1 : Le suivi médico-professionnel des salariés

Date de création de la fiche	**5 décembre 2018**
Date de dernière mise à jour de la fiche	**02/12/2024**
Nom du logiciel ou de l'application	uEgar (VAL SOLUTIONS) - CITRIX (PROGINOV)

Objectifs poursuivis

1. La santé au travail :
   - Surveillance de l'état de santé des travailleurs
   - Traçabilité et veille sanitaire
   - Conseil

2. Gestion du suivi individuel de l'état de santé du salarié :
   - Dossier administratif du salarié
   - Dossier médical interne (dont comptes-rendus médicaux)
   - Documents délivrés à l'issue des visites (aptitude, inaptitude, attestation de suivi)

3. Actions en milieu de travail, accompagnement en prévention primaire :
   - Etudes de postes
   - Comptes rendus d'intervention (exemples : métrologies, réunions, …)

4. La Prévention de la Désinsertion Professionnelle et du maintien en emploi
   - Fiche d'entretien prévention PDP
   - Le suivi accompagnement PDP
   - Autorisation contact avec l'entreprise

Catégories de personnes concernées

1. Salariés des entreprises adhérentes
2. Travailleurs non-salariés des entreprises adhérentes
3. Travailleurs indépendants

Catégories de données collectées

[X] **Etat-civil, identité, données d'identification, images**

Civilité, nom, prénoms, adresse, numéro de téléphone (fixe et/ou mobile), numéro de télécopie, adresses de courrier électronique, date de naissance, Identifiant National de Santé (INS), code interne de traitement permettant l'identification du client. Une copie d'un titre d'identité peut être conservée aux fins de preuve de l'exercice des droits légaux prévus par le RGPD ou pour répondre à une obligation légale.

[X] **Vie personnelle**

Vie maritale, nombre de personnes composant le foyer, nombre et âge du ou des enfant(s) au foyer, profession, domaine d'activité, catégorie socioprofessionnelle.

[X] **Autres catégories de données** :

1/ Organisation et suivi des visites médicales des salariés
Catégorie de suivi médical (SIG, SIA ou SIR), Date de la dernière visite médicale, Période de la prochaine visite médicale, Date de convocation, Heure de convocation, Heure d'arrivée à la visite, Nature de visite, Consultant, Motif d'absence, Historique de convocations, Historique des messages,

2/ Gestion du dossier médico-social du salarié
Social : type de handicap, date et taux IPP, date et catégorie invalidité, dossier Maison du Handicap, Habitat, Trajet, Finances, Enquête prévention de la désinsertion professionnelle
Médical : Biométrie, Fumeur, Stress, Pathologies, Traitements, Prescriptions, Résultats d'examens, Dosimétrie radiations ionisantes, fiches individuelles d'exposition Amiante, Accidents du travail, Maladies Professionnelles, Observations médicales, Restrictions d'aptitude, Vaccins, Tests immunitaires, Contraception, Grossesse, Antécédents personnels et familiaux, Sports, Voyages, Historique des visites médicales, Historique des avis d'aptitudes, inaptitudes et attestations de visites, Soins, Notes personnelles consultants, Notes partagées, Courriers

3/ Activités en milieu de travail
Etude de poste, métrologie, attestation de présence.

4/ Planning
Information date et heure du rendez vous

Des données sensibles sont-elles traitées ?

[x] Oui [ ] Non

Les Données de santé.

Durées de conservation des catégories de données

Données des salariés :
Conservation pendant 40 ans à compter de la dernière consultation (article R.4624-45-9 du Code du travail).
L'article R4624-18 du code du travail prévoit les cas de surveillance médicale renforcée. Des règles spécifiques de durée de conservation existent pour certains d'entre eux :
• Agents biologiques pathogènes : le dossier médical spécial est conservé 10 ans à compter de la cessation de l'exposition (article R 4426-9 du code du travail) ;
• Agents chimiques dangereux et agents chimiques dangereux cancérogènes, mutagènes et toxiques pour la reproduction : le dossier individuel est conservé pendant au moins 50 ans après la fin de la période d'exposition (article R 4412-55 du code du travail) ;
• Rayonnements ionisants : le dossier individuel est conservé pendant au moins 50 ans après la fin de la période d'exposition (article R 4451-90 du code du travail) ;
• Milieu hyperbare : le dossier médical est conservé pendant au moins 20 ans (article 35 du décret n°90-277 du 28 mars 1990 modifié) ;
• Amiante : le dossier est conservé 50 ans après la fin de la période d'exposition (article D 4412-95 du code du travail).
Pour simplifier la gestion des données, nous conservons les dossiers médicaux sans limitation de durée.

Catégories de destinataires des données

Destinataires internes

Personnes habilitées à traiter les données au sein de l'AST BTP

Organismes externes

Les entreprises adhérentes pour les documents issus des visites médicales (attestation de suivi, fiche d'aptitude inaptitude, mesures d'accompagnement)
DREETS, CARSAT, voire partenaires prévention : rapports et enquêtes anonymes

Sous-traitants

- Hébergement espace CITRIX : PROGINOV
- Logiciel uEgar : VAL SOLUTIONS
- Centre de formation des apprentis de Bourg en Bresse : formation Sauveteur Secouriste du Travail
- ADAKA : gestionnaire du site internet

Transferts des données hors UE

☐ Oui ☒ Non

Mesures de sécurité

☒ Contrôle d'accès des utilisateurs

- Données papier :
  - Alarme anti-intrusion au siège.
  - Verrouillage par badges numérotés au siège.
  - Clés (centres annexes)
  - Engagement individuel de réception et restitution des badges et clés (stockés dans les dossiers individuels des salariés, dans le bureau de l'assistante de direction);
  - Contrôle annuel dans tous les centres fixes des installations électriques et de protection incendie.

- Données informatiques :
  - Identification des utilisateurs dans le réseau (identification/mot de passe, changement obligatoire tous les 12 mois)
  - Identification des utilisateurs du progiciel (identification/mot de passe, changement obligatoire tous les 12 mois)

Accès à l'hébergement CITRIX :

La connexion des utilisateurs du Service de Santé au Travail se fait par deux techniques :
a. Accès par le réseau privé MPLS du Service et gestion des connexions par le logiciel CITRIX
b. Accès par Internet : dans ce cas, une authentification forte par jeton est requise pour se connecter au Système d'Information
L'étanchéité du réseau est assurée par la séparation logique en VLAN (réseaux virtuels) des différentes zones de l'architecture
- Un ou plusieurs VLAN dédié par client suivant les besoins
- Un VLAN d'administration du réseau « santé »
- des pares-feux qui assurent le filtrage de toutes les connexions.

Accès hiérarchisé aux données uEgar depuis l'espace sécurité CITRIX :

1) Définition de cinq types de données hiérarchisées : données administratives, données socio-professionnelles, données médicales personnelles, données médicales partagées réservées à l'équipe de consultants (médecins, infirmières), données médicales réservées à un consultant (celui qui les a créés),
2) Définition des types d'utilisateurs (Médecins du travail, Médecins spécialistes, Infirmiers(es), Secrétaires médicales, Personnel administratif, Psychologues, Assistants sociaux, Personnels techniques, Préventeurs/IPRP)
3) Les droits d'accès sont définis selon différents axes : accès aux menus, accès aux dossiers, accès aux objets (pathologies, visites, conclusions)
4) Les profils définissent 2 sortes de droits : L'accès aux menus et L'accès aux objets (pathologies, visites, conclusions, soins, expositions individuelles, suivi PDP, données sociales)
5) La combinaison par paramétrage de ces différents éléments permet de déterminer de façon précise les droits d'accès de chaque utilisateur à chaque type de données et de plus permet de déterminer le mode d'accès aux données autorisé (lecture, création, mise à jour, suppression)

Accès à l'espace connecté salarié : accès délivré par l'entreprise à ses salariés (identification par identifiant et mot de passe)

[X] Mesures de traçabilité

Le progiciel uEgar trace les opérations suivantes :
1) Les connexions utilisateurs à l'application
2) L'historique des accès au dossier médical et le type d'accès (Accès Consultant, Auxiliaire, Social). ~~Seul le médecin référent peut consulter l'historique des accès au dossier médical~~
3) Les ajouts, modifications, suppressions de données, à l'exception des données administratives (factures, règlements, lettrages)
CITRIX : journalisation des accès des utilisateurs (identifiant, date et heure de connexion)

[X] Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

L'ensemble des logiciels de la plateforme est mis à jour au fur et à mesure de la disponibilité des correctifs de sécurité et des évolutions fonctionnelles et techniques chez les éditeurs de logiciels.
L'ensemble des accès est filtré par des Firewall, des logiciels antivirus, anti spams, anti amorçage, etc. qui sont actifs sur les différents serveurs de données et d'accès à Internet
La réception et l'envoi de mails sont contrôlés par Antivirus, anti spams, etc…

[X] Sauvegarde des données

PROGINOV a choisi de stocker toutes les données sur des baies de stockage haute performance connectées en fibre optique. Un réseau de stockage dédié aux clients santé a été créé et l'utilisation d'unité de stockage logique par client permet l'étanchéité totale entre eux.
Les baies de stockage sont systématiquement doublées. Les données sont dupliquées en temps réel
Un « cluster » (groupe de serveurs) de Serveurs de sauvegarde pilote une bandothèque pour la gestion centralisée des sauvegardes.
Le cycle de Sauvegarde est quotidien :
• Bureautique et Messagerie : incrémentale quotidienne sur 20 jours + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort
• Base de données : incrémentale quotidienne sur 31 jours et complète 27 quinzaines + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort

[X] Chiffrement des données

Les données transitant sur le réseau entre les postes de travail et les serveurs sont cryptés (cryptage SSL).
Pour le transfert des résultats d'examens médicaux : messagerie sécurisée MonSisra.

Pour le transfert des dossiers médicaux d'un SPST à un autre : envoi en recommandé avec accusé de réception après accord signé du salarié.

[X] Contrôle des sous-traitants

Les contrats établis entre le Service de Santé au Travail et PROGINOV décrivent toutes les prestations et mesures de sécurité et de confidentialité. Les Salariés de l'Hébergeur PROGINOV sont astreints au Secret professionnel n'ont pas d'accès aux données gérées par le progiciel uEgar.
Les contrats établis entre le Service de Santé au Travail et VAL SOLUTIONS décrivent les prestations et mesures de sécurité et de confidentialité du Progiciel uEgar

Maintenance du Progiciel uEgar :

1) Une clause de confidentialité a été signée entre les deux parties.
2) Les salariés de VAL SOLUTIONS sont soumis au secret professionnel par leur contrat de travail et les engagements contenus dans la charte informatique de VAL SOLUTIONS.

[X] Autres mesures :

PROGINOV dispose depuis le 3 novembre 2014, de l'agrément par le Ministère des affaires sociales, de la santé et des droits des femmes, conformément au décret n°2006-6 du 4 janvier 2006, en tant qu'hébergeur de données de santé à caractère personnel. Cet agrément vaut pour toute « prestation d'hébergement de données de santé à caractère personnel collectées au moyen d'applications fournies par les clients à des fins de suivi médical ».
Par ailleurs PROGINOV a engagé une démarche visant à la conformité à la norme ISO 27001 et au code des bonnes pratiques préconisées par la norme ISO 27002.
L'ensemble des mesures prises en vue de la protection d'accès, l'intégrité aux données et la sauvegarde des données sont décrits dans un document intitulé « Santé annexe 2 : présentation du service d'Hébergement »

Protection d'accès au Système d'Information du Service de Santé au Travail
• Protection et intégrité physique
Le Système d'Information est dupliqué en temps réel, dans 2 « Datacenters » indépendants aussi bien en termes d'alimentation électrique, de climatisation, que de lignes de communications situées au 36 Rue de la Guillauderie 44118 LA CHEVROLIERE et au 2 rue Gustave Eiffel 44118 LA CHEVROLIERE. La continuité de service est assurée par la redondance de l'ensemble des équipements et services.

Les locaux de PROGINOV sont sécurisés sur le périmètre par un grillage autour de l'ensemble du terrain, un contrôle par barrière infrarouge relié au système d'alarme et au PC de surveillance.

Le contrôle d'accès aux locaux se fait par un système de badge individuel qui contrôle et enregistre les accès des personnes (horaires autorisés ou non, types de locaux autorisés ou non). L'extérieur des locaux est filmé en vidéosurveillance 24h/24 et 7jrs/7. Les images sont conservées jusqu'à 30 jours.

Un document décrit les responsabilités respectives du Service de Santé au Travail, de VAL SOLUTIONS et de PROGINOV dans les domaines de la protection des données, de leur intégrité et de leur confidentialité. Ce document est intitulé « Santé Annexe 1 : Matrice des responsabilités »

Activité 2 : Les entreprises adhérentes

Date de création de la fiche	**5 décembre 2018**
Date de dernière mise à jour de la fiche	**2 décembre 2024**
Nom du logiciel ou de l'application *(si pertinent)*	uEgar (VAL SOLUTIONS) - CITRIX (PROGINOV)

Objectifs poursuivis

La santé au travail :

- Surveillance de l'état de santé des travailleurs
- Traçabilité et veille sanitaire
- Conseils en prévention primaire
- Actions en entreprises

Gestion de la relation avec l'entreprise :

- Adhésion
- Déclaration des effectifs
- Convocation des salariés
- Demandes de visites

Actions en milieu de travail :

- Fiches d'entreprises
- Etudes de postes
- Formulaires d'inscription et de présence aux sessions d'information collectives
- Comptes-rendus d'intervention (métrologies, réunions, accompagnements…)

Catégories de personnes concernées

Adhérents : personne morale (entreprises et agences de travail temporaire)
Salariés des entreprises adhérentes
Travailleurs non-salariés des entreprises adhérentes
Travailleurs indépendants
Cabinet comptable externe des entreprises
Personnel de l'AST BTP de l'Ain

Catégories de données collectées

[X] **Etat-civil, identité, données d'identification, images**

Nom, prénom, téléphone du dirigeant de l'entreprise adhérente, d'un correspondant du cabinet comptable,
Nom, prénom, date de naissance des salariés des entreprises adhérentes et agences de travail temporaire
Nom, prénom, fonction, téléphone professionnel, email professionnel du personnel AST BTP de l'Ain

[X] **Vie professionnelle**

Salarié : emploi déclaré par l'employeur, type de contrat, date de début de poste, date de fin de poste, risques déclarés par l'employeur

Des données sensibles sont-elles traitées ?

☐ Oui ☒ Non

Durées de conservation des catégories de données

Pour simplifier la gestion des données nous conservons les dossiers des entreprises qui sont informatisées sans limitation de durée (contrat d'adhésion, fiche d'entreprise, étude de poste…).

Catégories de destinataires des données

Destinataires internes

Personnel de l'AST BTP de l'Ain

Organismes externes

La DREETS, la CARSAT, l'OPPBTP, autres services de santé.

Sous-traitants

- Hébergement, espace CITRIX : PROGINOV
- Logiciel uEgar : VAL SOLUTIONS
- Centre de formation des apprentis de Bourg en Bresse : formation Sauveteur Secouriste du Travail
- ADAKA : gestionnaire du site internet
- ADDEO : créateur du site internet
- MonSisra : messagerie sécurisée

Transferts des données hors UE

☐ Oui ☒ Non

Mesures de sécurité (à compléter par l'entreprise)

☒ Contrôle d'accès des utilisateurs

Identification des utilisateurs dans le réseau (identification/mot de passe, changement obligatoire tous les 12 mois)
Identification des utilisateurs du progiciel (identification/mot de passe, changement obligatoire tous les 12 mois)

Accès à l'hébergement CITRIX :
La connexion des utilisateurs du Service de Santé au Travail se fait par deux techniques :
a. Accès par le réseau privé MPLS du Service et gestion des connexions par le logiciel CITRIX
b. Accès par Internet : dans ce cas, une authentification forte par jeton est requise pour se connecter au Système d'Information

L'étanchéité du réseau est assurée par la séparation logique en VLAN (réseaux virtuels) des différentes zones de l'architecture
• Un ou plusieurs VLAN dédié par client suivant les besoins
• Un VLAN d'administration du réseau « santé »
• des pares-feux qui assurent le filtrage de toutes les connexions.

Accès hiérarchisé aux données uEgar depuis l'espace sécurité CITRIX :

1) Définition de cinq types de données hiérarchisées : données administratives, données socio-professionnelles, données médicales personnelles, données médicales partagées réservées à l'équipe de consultants (médecins, infirmières), données médicales réservées à un consultant (celui qui les a créés),
2) Définition des types d'utilisateurs (Médecins du travail, Médecins spécialistes, Infirmiers(es), Secrétaires médicales, Personnel administratif, Psychologues, Assistants sociaux, Personnels techniques, Préventeurs/IPRP)
3) Les droits d'accès sont définis selon différents axes : accès aux menus, accès aux dossiers, accès aux objets (pathologies, visites, conclusions)
4) Les profils définissent 2 sortes de droits : L'accès aux menus et L'accès aux objets (pathologies, visites, conclusions, soins, expositions individuelles, suivi PDP, données sociales)
5) La combinaison par paramétrage de ces différents éléments permet de déterminer de façon précise les droits d'accès de chaque utilisateur à chaque type de données et de plus permet de déterminer le mode d'accès aux données autorisé (lecture, création, mise à jour, suppression)

Accès au portail adhérent

Identification des entreprises adhérentes par un lien de connexion (URL) transmis par mail et un mot de passe provisoire délivrés par l'AST BTP de l'Ain (nécessité pour l'adhérent de modifier son mot de passe à la première connexion).

Sécurisation par VAL SOLUTIONS et PROGINOV

[X] Mesures de traçabilité

Le progiciel uEgar trace les opérations suivantes :
1) Les connexions utilisateurs à l'application
2) L'historique des accès au dossier médical (à partir de la version v2.1.1) et le type d'accès (Accès Consultant, Auxiliaire, Social). ~~Seul le médecin référent peut consulter l'historique des accès au dossier médical~~
3) Les ajouts, modifications, suppressions de données, à l'exception des données administratives (factures, règlements, lettrages)
CITRIX : journalisation des accès des utilisateurs (identifiant, date et heure de connexion)

[X] Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

L'ensemble des logiciels de la plateforme est mis à jour au fur et à mesure de la disponibilité des correctifs de sécurité et des évolutions fonctionnelles et techniques chez les éditeurs de logiciels.
L'ensemble des accès est filtré par des Firewall, des logiciels antivirus, anti spams, anti amorçage, etc. qui sont actifs sur les différents serveurs de données et d'accès à Internet
La réception et l'envoi de mails sont contrôlés par Antivirus, anti spams, etc…

[X] Sauvegarde des données

PROGINOV a choisi de stocker toutes les données sur des baies de stockage haute performance connectées en fibre optique. Un réseau de stockage dédié aux clients santé a été créé et l'utilisation d'unité de stockage logique par client permet l'étanchéité totale entre eux.
Les baies de stockage sont systématiquement doublées. Les données sont dupliquées en temps réel

Un « cluster » (groupe de serveurs) de Serveurs de sauvegarde pilote une bandothèque pour la gestion centralisée des sauvegardes.

Le cycle de Sauvegarde est quotidien :
• Bureautique et Messagerie : incrémentale quotidienne sur 20 jours + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort
• Base de données : incrémentale quotidienne sur 31 jours et complète 27 quinzaines + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort

[X] Chiffrement des données

Les données transitant sur le réseau entre les postes de travail et les serveurs sont cryptés (cryptage SSL)

[X] Contrôle des sous-traitants

Les contrats établis entre le Service de Santé au Travail et PROGINOV décrivent toutes les prestations et mesures de sécurité et de confidentialité. Les Salariés de l'Hébergeur PROGINOV sont astreints au Secret professionnel n'ont pas d'accès aux données gérées par le progiciel uEgar.
Les contrats établis entre le Service de Santé au Travail et VAL SOLUTIONS décrivent les prestations et mesures de sécurité et de confidentialité du Progiciel uEgar

Maintenance du Progiciel uEgar :
1) Une clause de confidentialité a été signée entre les deux parties.
2) Les salariés de VAL SOLUTIONS sont soumis au secret professionnel par leur contrat de travail et les engagements contenus dans la charte informatique de VAL SOLUTIONS.

[X] Autres mesures :

PROGINOV dispose depuis le 3 novembre 2014, de l'agrément par le Ministère des affaires sociales, de la santé et des droits des femmes, conformément au décret n°2006-6 du 4 janvier 2006, en tant qu'hébergeur de données de santé à caractère personnel. Cet agrément vaut pour toute « prestation d'hébergement de données de santé à caractère personnel collectées au moyen d'applications fournies par les clients à des fins de suivi médical ».
Par ailleurs PROGINOV a engagé une démarche visant à la conformité à la norme ISO 27001 et au code des bonnes pratiques préconisées par la norme ISO 27002.
L'ensemble des mesures prises en vue de la protection d'accès, l'intégrité aux données et la sauvegarde des données sont décrits dans un document intitulé « Santé annexe 2 : présentation du service d'Hébergement »

Protection d'accès au Système d'Information du Service de Santé au Travail

• Protection et intégrité physique

Le Système d'Information est dupliqué en temps réel, dans 2 « Datacenters » indépendants aussi bien en termes d'alimentation électrique, de climatisation, que de lignes de communications situées au 36 Rue de la Guillauderie 44118 LA CHEVROLIERE et au 2 rue Gustave Eiffel 44118 LA CHEVROLIERE. La continuité de service est assurée par la redondance de l'ensemble des équipements et services.

Les locaux de PROGINOV sont sécurisés sur le périmètre par un grillage autour de l'ensemble du terrain, un contrôle par barrière infrarouge relié au système d'alarme et au PC de surveillance.

Le contrôle d'accès aux locaux se fait par un système de badge individuel qui contrôle et enregistre les accès des personnes (horaires autorisés ou non, types de locaux autorisés ou non). L'extérieur des locaux est filmé en vidéosurveillance 24h/24 et 7jrs/7. Les images sont conservées jusqu'à 30 jours.

De plus, il y a un destructeur interne de documents dans chaque centre.

Activité 3 : Les fournisseurs

Date de création de la fiche	**07 septembre 2018**
Date de dernière mise à jour de la fiche	**6 juin 2023**
Nom du logiciel ou de l'application *(si pertinent)*	**SAGE**

Objectifs poursuivis

- Opérations administratives liées aux contrats, aux commandes, aux réceptions, aux factures, aux règlements, à la comptabilité pour ce qui a trait à la gestion des comptes fournisseurs ;
- Établissement des titres de paiement (virements, chèques, espèces) ;
- Fourniture de sélections de fournisseurs pour les besoins de l'entreprise ;

Catégories de personnes concernées

1. Fournisseurs de l'entreprise

Catégories de données collectées

[X] **Etat-civil, identité, données d'identification, images**

Nom ou raison sociale, prénoms, adresse (siège social, lieu de facturation), code d'identification comptable, téléphone, fax, adresse de courrier électronique, numéro SIREN, code NAF, Numéro de TVA intracommunautaire,

[X] **Vie professionnelle**

Profession, activité.

[X] **Autres catégories de données** *(précisez)* :

Eléments de facturation et de règlement :

- les bons de commandes et les factures, conditions de livraison ;
- paiement, conditions et modalités de règlement ;
- impayés, avoirs, reçus.

Des données sensibles sont-elles traitées ?

[ ] Oui [X] Non

Durées de conservation des catégories de données

Jusqu'à 10 ans (obligations légales et règlementaires en vigueur).

Catégories de destinataires des données

Destinataires internes

1. Directeur/trice
2. Responsable Administratif et Financier
3. Assistante de direction

Organismes externes

1. Personnes chargées du contrôle (commissaire aux comptes, expert-comptable)
2. Organismes financiers teneurs des comptes mouvementés (banques)

Transferts des données hors UE

☐ Oui ☒ Non

Mesures de sécurité

☒ Contrôle d'accès des utilisateurs

L'accès aux fiches fournisseurs informatisées se fait sur les logiciels de Comptabilité et Moyens de Paiement SAGE accessible par le Responsable Administratif et Financier sur son ordinateur. Ceux-ci sont protégés par deux mots de passe :

- un pour l'ouverture du PC sur lequel est installé le logiciel de Comptabilité et Moyens de Paiements
- un à l'ouverture des logiciels

Pour les règlements par virement des factures fournisseurs via notre banque par internet, protection avec un lecteur de carte à puce et un code d'accès.
Les factures fournisseurs N à N-2 sont classées au siège de Bourg-en-Bresse, dans le bureau du RAF ; les autres sont archivées dans le local archives. Ces accès sont fermés à clé et sécurisés par une alarme.

☒ Mesures de protection des logiciels

Le logiciel de Comptabilité et Moyens de Paiements sont protégés par un anti-virus (F-SECURE) mis à jour automatiquement et un Firewall.

☒ Sauvegarde des données

Les données du logiciel de Comptabilité sont sauvegardées tous les jours chez l'hébergeur externe PROGINOV.

PROGINOV a choisi de stocker toutes les données sur des baies de stockage haute performance connectées en fibre optique. Un réseau de stockage dédié aux clients santé a été créé et l'utilisation d'unité de stockage logique par client permet l'étanchéité totale entre eux.

Les baies de stockage sont systématiquement doublées. Les données sont dupliquées en temps réel
Un « cluster » (groupe de serveurs) de Serveurs de sauvegarde pilote une bandothèque pour la gestion centralisée des sauvegardes.

Le cycle de Sauvegarde est quotidien :

- Bureautique et Messagerie : incrémentale quotidienne sur 20 jours + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort
- Base de données : incrémentale quotidienne sur 31 jours et complète 27 quinzaines + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort.

☐ Chiffrement des données

Les données transitant sur le réseau entre les postes de travail et les serveurs sont cryptées (cryptage SSL)

☒ Autres mesures :

- Signature d'un engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel ou sensible.
- Destructeur interne de documents dans chaque centre.
- Assurance en responsabilité civile et professionnelle de l'AST BTP et des fournisseurs, prestataires de service, voire sous-traitants.

PROGINOV dispose depuis le 3 novembre 2014, de l'agrément par le Ministère des affaires sociales, de la santé et des droits des femmes, conformément au décret n°2006-6 du 4 janvier 2006, en tant qu'hébergeur de données de santé à caractère personnel. Cet agrément vaut pour toute « prestation d'hébergement de données de santé à caractère personnel collectées au moyen d'applications fournies par les clients à des fins de suivi médical ».
Par ailleurs PROGINOV a engagé une démarche visant à la conformité à la norme ISO 27001 et au code des bonnes pratiques préconisées par la norme ISO 27002.
L'ensemble des mesures prises en vue de la protection d'accès, l'intégrité aux données et la sauvegarde des données sont décrits dans un document intitulé « Santé annexe 2 : présentation du service d'Hébergement »

Protection d'accès au Système d'Information du Service de Santé au Travail

- Protection et intégrité physique

Le Système d'Information est dupliqué en temps réel, dans 2 « Datacenters » indépendants aussi bien en termes d'alimentation électrique, de climatisation, que de lignes de communications situées au 36 Rue de la Guillauderie 44118 LA CHEVROLIERE et au 2 rue Gustave Eiffel 44118 LA CHEVROLIERE. La continuité de service est assurée par la redondance de l'ensemble des équipements et services.

Les locaux de PROGINOV sont sécurisés sur le périmètre par un grillage autour de l'ensemble du terrain, un contrôle par barrière infrarouge relié au système d'alarme et au PC de surveillance.

Le contrôle d'accès aux locaux se fait par un système de badge individuel qui contrôle et enregistre les accès des personnes (horaires autorisés ou non, types de locaux autorisés ou non). L'extérieur des locaux est filmé en vidéosurveillance 24h/24 et 7jrs/7. Les images sont conservées jusqu'à 30 jours.

Un document décrit les responsabilités respectives du Service de Santé au Travail, de VAL SOLUTIONS et de PROGINOV dans les domaines de la protection des données, de leur intégrité et de leur confidentialité. Ce document est intitulé « Santé Annexe 1 : Matrice des responsabilités »

Activité 4 : La comptabilité générale

Date de création de la fiche	**13 décembre 2019**
Date de dernière mise à jour de la fiche	**2 décembre 2024**
Nom du logiciel ou de l'application *(si pertinent)*	**SAGE – uEgar (**VAL SOLUTIONS**)**

Objectifs poursuivis

1) Effectuer les opérations liées aux adhésions, aux contrats, aux commandes, aux réceptions, aux factures, aux règlements, à la comptabilité
2) Gérer les cotisations et les factures
3) Gérer les adhésions, les suspensions et les radiations des entreprises adhérentes
4) Etablir les états de synthèse et calculer et déclarer les impôts et taxes
5) Etablir les titres de paiement (Chèques, virements, paiement carte bleue, prélèvements)
6) Effectuer les Reportings pour les assemblées générales, le conseil d'administration et la commission de contrôle, la Direction Générale du Travail (DGT)
7) Assurer le suivi du budget et la production du compte administratif

Catégories de personnes concernées

1) Entreprises adhérentes (personnes morales + personnes physiques)
2) Contacts de gestion des entreprises adhérentes
3) Entreprises fournisseurs et prestataires de service
4) Personnel du SPSTI

[X] **Etat-civil, identité, données d'identification, images**

Raison sociale, téléphone, email, fax et nom, prénom et fonction des contacts des entreprises adhérentes.
Raison sociale, téléphone, email, fax et contacts des fournisseurs et prestataires de service.
Activité, Code NAF, N° SIRET, N°PAJE ou n° CESU, Adresse de facturation, Adresse de convocation, nombre de salariés à prendre en charge, montant (DADS/DSN)

Des données sensibles sont-elles traitées ?

[ ] Oui [X] Non

Durée de conservation des catégories de données

10 ans à compter de la clôture du livre ou du registre.

Catégories de destinataires des données

Destinataires internes

Services comptables et organismes habilités à recevoir les données en vertu des règles de comptabilité.

Destinataires externes

1. Expert-comptable ;
2. Commissaire aux comptes ;
3. Organismes financiers ;
4. Membres du conseil d'administration et de la commission de contrôle ;
5. Organismes d'Etat : Trésor Public, DREETS, DGT …

Sous-traitants

- **PROGINOV, Hébergeur** pour la bureautique dont la paye et la comptabilité et le logiciel métier uEgar.
- **APOGEA, maintenance** des produits SAGE (compta-Paie-moyens de paiement).
- **VAL SOLUTIONS, maintenance** des produits uEgar.

Transferts des données hors UE

☐ Oui ☒ Non

Mesures de sécurité

☒ Contrôle d'accès des utilisateurs

L'accès au logiciel de Comptabilité n'est accessible que par le Responsable Administratif et Financier et la Directrice sur l'ordinateur du RAF. Le logiciel est hébergé sur un serveur chez hébergeur agrée PROGINOV.
Celui-ci est protégé par deux mots de passe :

- un pour l'ouverture du PC sur lequel est installé le logiciel de Comptabilité
- un à l'ouverture du logiciel

☒ Mesures de traçabilité

Le fichier de Comptabilité (**AST01.mae**) n'est accessible que par le Responsable Administratif et Financier. Celui est stocké sur le serveur PROGINOV dans le répertoire P:\ast01_b_sve\Sage\Compta

Possibilité d'accès par la direction qui détient les mots de passe.

☒ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Le logiciel de Comptabilité est protégé par un anti-virus (F-SECURE) sur le poste en local mis à jour automatiquement et un Firewall, et protégé sur le serveur hébergé chez PROGINOV.

☒ Sauvegarde des données

Les données du logiciel de Comptabilité sont sauvegardées tous les jours chez l'hébergeur externe PROGINOV.

PROGINOV a choisi de stocker toutes les données sur des baies de stockage haute performance connectées en fibre optique. Un réseau de stockage dédié aux clients santé a été créé et l'utilisation d'unité de stockage logique par client permet l'étanchéité totale entre eux.

Les baies de stockage sont systématiquement doublées. Les données sont dupliquées en temps réel
Un « cluster » (groupe de serveurs) de Serveurs de sauvegarde pilote une bandothèque pour la gestion centralisée des sauvegardes.

Le cycle de Sauvegarde est quotidien :

- Bureautique et Messagerie : incrémentale quotidienne sur 20 jours + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort
- Base de données : incrémentale quotidienne sur 31 jours et complète 27 quinzaines + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort

☒ Chiffrement des données

Les données transitant sur le réseau entre les postes de travail et les serveurs sont cryptées (cryptage SSL)
Logiciel installé en monoposte

☒ Contrôle des sous-traitants

Les mises à jour pour la maintenance du logiciel SAGE sont réalisées par la société APOGEA. Le contrôle est effectué par une identification préalable auprès de PROGINOV, qui autorise l'accès.

[X] Autres mesures :
Signature d'un engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel ou sensible.
Destructeur interne de documents dans chaque centre.

Activité 5 : La paie

Date de création de la fiche	**13 décembre 2019**
Date de dernière mise à jour de la fiche	**2 décembre 2024**
Nom du logiciel ou de l'application *(si pertinent)*	**SAGE**

Objectifs poursuivis

- Calcul et paiement des rémunérations et accessoires et des frais professionnels ;
- Déclarations et versements à l'administration fiscale et aux organismes de protection sociale, de retraite et de prévoyance ;
- Tenue des comptes individuels relatifs au Plan Epargne d'Entreprise ;
- Fourniture des informations et réalisation des états relatifs à la situation du personnel permettant de satisfaire à des obligations légales (telles que la tenue du registre unique du personnel) ;
- Fourniture des écritures de la paie à la comptabilité.

Catégories de personnes concernées

Les salariés

Catégories de données collectées

[X] **Etat-civil, identité, données d'identification, images**

Nom, nom marital, prénoms, sexe, date et lieu de naissance, numéro de sécurité sociale dans les conditions fixées par le décret n° 91-1404 du 27 décembre 1991 (déclarations, calculs de cotisations et versements destinés aux organismes sociaux et fiscaux) ou par l'article L. 3341-6 du code du travail (livret d'épargne salariale), adresse ; numéros attribués par les organismes d'assurances sociales, de retraite et de prévoyance, nationalité (Français, étranger).

[X] **Vie personnelle**

Situation matrimoniale, enfants à charge.

[X] **Vie professionnelle**

Lieu de travail, date d'entrée et de sortie dans l'entreprise, ancienneté, emploi occupé et coefficient hiérarchique, nature du contrat de travail.

[X] **Informations d'ordre économique et financier**

Régime et base de calcul de la rémunération ; nature, taux et base des cotisations sociales, congés et absences donnant lieu à retenues déductibles ou indemnisables ainsi que toute retenue légalement opérée par l'employeur, frais professionnels, mode de règlement, identité bancaire ou postale.

Des données sensibles sont-elles traitées ?

[X] Oui [ ] Non

Si oui, lesquelles ? : Numéro de sécurité

Durées de conservation des catégories de données

La durée de conservation des informations n'excède pas celle prévue par les dispositions légales.
Les informations nécessaires à l'établissement des droits du personnel, notamment des droits à la retraite, et les bulletins de paye sont conservés sans limitation de durée.

Catégories de destinataires des données

Destinataires internes

Directeur/trice du service
Responsable Administratif et Financier

Organismes externes

1. Organismes gérant les différents systèmes d'assurances sociales, d'assurances chômage, de retraite et de prévoyance.
2. Organismes publics et administrations légalement habilités à recevoir les données ;
3. Organismes financiers intervenant dans la gestion des comptes de l'entreprise et du salarié.

Sous-traitants

- **PROGINOV, Hébergeur** pour la bureautique dont la paye et la comptabilité et le logiciel métier uEgar.
- **APOGEA, maintenance** des produits SAGE (compta-Paie-moyens de paiement).

Transferts des données hors UE

☐ Oui ☒ Non

Mesures de sécurité

☒ Contrôle d'accès des utilisateurs

L'accès au logiciel de Paie n'est accessible que par le Responsable Administratif et Financier et la Directrice sur l'ordinateur du RAF . Le logiciel est hébergé sur un serveur chez hébergeur agrée PROGINOV.
Celui-ci est protégé par trois mots de passe :

- un pour l'ouverture du PC sur lequel est installé le logiciel de Paie
- un à l'ouverture du logiciel de Paie
- un à l'ouverture du fichier de Paie.

Possibilité d'accès par la Direction qui a connaissance des mots de passe.

☒ Mesures de traçabilité

Le fichier de Paie (**paie_ASTBTP.prh**) n'est accessible que par le Responsable Administratif et Financier. Celui-ci est stocké sur le serveur PROGINOV dans le répertoire P:\ast01_b_sve\Sage\Paie

☒ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Le logiciel de Comptabilité est protégé par un anti-virus (F-SECURE) sur le poste en local mis à jour automatiquement et un Firewall, et protégé sur le serveur hébergé chez PROGINOV.

☒ Sauvegarde des données

Les données du logiciel de paye sont sauvegardées tous les jours chez l'hébergeur externe PROGINOV.

PROGINOV a choisi de stocker toutes les données sur des baies de stockage haute performance connectées en fibre optique. Un réseau de stockage dédié aux clients santé a été créé et l'utilisation d'unité de stockage logique par client permet l'étanchéité totale entre eux.

Les baies de stockage sont systématiquement doublées. Les données sont dupliquées en temps réel

Un « cluster » (groupe de serveurs) de Serveurs de sauvegarde pilote une bandothèque pour la gestion centralisée des sauvegardes.

Le cycle de Sauvegarde est quotidien :

- Bureautique et Messagerie : incrémentale quotidienne sur 20 jours + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort
- Base de données : incrémentale quotidienne sur 31 jours et complète 27 quinzaines + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort

[X] Chiffrement des données

Les données transitant sur le réseau entre les postes de travail et les serveurs sont cryptés (cryptage SSL)

[X] Contrôle des sous-traitants

~~Pas de sous-traitant.~~ Les paies sont faites en interne. Les mises à jour pour la maintenance du logiciel SAGE sont réalisées par la société APOGEA. Le contrôle est effectué par une identification préalable auprès de PROGINOV, qui autorise l'accès.

[X] Autres mesures :

- Signature d'un engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel ou sensible.
- Information écrite de l'AST BTP à chaque salarié "Traitement des données personnelles – Gestion du personnel et de la paye".
- Destructeur interne de documents.
- Archivage des éléments de payes papier (actuelles et anciens salariés) sont stockés au siège sécurisé par le badge et l'alarme.
- Les accès et mots de passe sont également détenus par la Direction

PROGINOV dispose depuis le 3 novembre 2014, de l'agrément par le Ministère des affaires sociales, de la santé et des droits des femmes, conformément au décret n°2006-6 du 4 janvier 2006, en tant qu'hébergeur de données de santé à caractère personnel. Cet agrément vaut pour toute « prestation d'hébergement de données de santé à caractère personnel collectées au moyen d'applications fournies par les clients à des fins de suivi médical ».
Par ailleurs PROGINOV a engagé une démarche visant à la conformité à la norme ISO 27001 et au code des bonnes pratiques préconisées par la norme ISO 27002.
L'ensemble des mesures prises en vue de la protection d'accès, l'intégrité aux données et la sauvegarde des données sont décrits dans un document intitulé « Santé annexe 2 : présentation du service d'Hébergement »

Protection d'accès au Système d'Information du Service de Santé au Travail

- Protection et intégrité physique

Le Système d'Information est dupliqué en temps réel, dans 2 « Datacenters » indépendants aussi bien en termes d'alimentation électrique, de climatisation, que de lignes de communications situées au 36 Rue de la Guillauderie 44118 LA CHEVROLIERE et au 2 rue Gustave Eiffel 44118 LA CHEVROLIERE. La continuité de service est assurée par la redondance de l'ensemble des équipements et services.

Les locaux de PROGINOV sont sécurisés sur le périmètre par un grillage autour de l'ensemble du terrain, un contrôle par barrière infrarouge relié au système d'alarme et au PC de surveillance.

Le contrôle d'accès aux locaux se fait par un système de badge individuel qui contrôle et enregistre les accès des personnes (horaires autorisés ou non, types de locaux autorisés ou non). L'extérieur des locaux est filmé en vidéosurveillance 24h/24 et 7jrs/7. Les images sont conservées jusqu'à 30 jours.

Activité 6 : Les ressources humaines

Date de création de la fiche	**07 septembre 2018**
Date de dernière mise à jour de la fiche	**2 décembre 2024**
Nom du logiciel ou de l'application *(si pertinent)*	

Objectifs poursuivis

- **Traitement des recrutements**
- **Gestion administrative du personnel**
- **Mise à disposition du personnel d'outils de travail : informatiques, téléphoniques etc…**
- **Gestion des compétences et des carrières**
- **Gestion des représentants du personnel**

Catégories de personnes concernées

1. Salariés de l'entreprise et autres
2. Stagiaires
3. Candidats à l'embauche

Catégories de données collectées

[X] **Etat-civil, identité, données d'identification, images du candidat à l'embauche ou employés**

Nom, prénom, photographie (facultatif), sexe, date et lieu de naissance, nationalité, coordonnées, parcours professionnel (CV), recommandations, informations diverses éventuellement contenues dans le CV et la lettre de motivation (situation familiale, loisirs, etc.), permis de conduire, coordonnées des personnes à prévenir etc …

[X] **Autres catégories de données** *:*

- **Gestion administrative** :

- Dossier professionnel
- Annuaires internes et organigrammes
- Dotations individuelles : équipements, véhicules dont carnet de bord, badges autoroute, carte paiement…
- Suivi administratif des visites médicales et des déclarations d'AT ou MP : coordonnées du médecin du travail, dates des visites, attestations délivrées : suivi, aptitude ou inapte, propositions d'adaptation du poste de travail ou à un autre poste de travail, date du dernier jour de travail, date de reprise, motif de l'arrêt…
- Aspects sociaux : identité de l'employé et de ses ayants droit ou ouvrants droit, prévoyance et couverture des frais de santé, revenus, avantages dont avantage en nature et prestations demandés et servis ;

- **Gestion des compétences et des carrières :**

Entretien professionnel, validation des acquis de l'expérience professionnelle, formation professionnelle (suivi des demandes, organisation des sessions de formation, élaboration et suivi du plan de formation…), gestion de la mobilité, fiche de poste etc… :

- Embauche /Recrutement : Date et conditions du contrat de travail

- Modifications apportées à la situation professionnelle de l'employé : Date, objet et motif. Sanctions disciplinaires à l'exclusion de celles consécutives à des faits amnistiés

- Évaluation professionnelle de l'employé : dates des entretiens professionnels, identité de l'évaluateur, compétences professionnelles de l'employé, éventuellement objectifs assignés et résultats obtenus, appréciation des aptitudes professionnelles sur la base de critères objectifs et présentant un lien direct et nécessaire avec l'emploi occupé, souhait de l'employé en termes d'emploi, observations et souhaits formulés par l'employé, prévisions d'évolution de carrière

- Formation : diplômes, certificats et attestations, langues étrangères pratiquées, suivi des demandes de formation professionnelle et des périodes de formation effectuées, organisation des sessions de formation, évaluation des connaissances et des formations

- Validation des acquis de l'expérience : date de la demande de la VAE qualification concernée, expériences soumises à validation, validation (oui/non), date de la décision

- **Organisation du travail :**

- Annuaires internes et organigrammes : nom, prénom, photographie (facultatif), fonction, coordonnées professionnelles, le cas échéant, formation et réalisations professionnelles
- Agendas professionnels : dates, lieux et heures des rendez-vous professionnels, objet, personnes présentes
- Tâches des personnels : Fiche de poste
- Gestion des dotations individuelles : cf Gestion administrative
- Messagerie électronique : carnet d'adresses, comptes individuels

- **Gestion des représentants du personnel**

- Élections professionnelles : établissement de la liste électorale (identité des électeurs, âge, ancienneté, collège), gestion des candidatures et publication des résultats (identité des candidats, mandats concernés, nombre et pourcentage de suffrages obtenus, identité des personnels élus et, le cas échéant, appartenance syndicale des élus) ;
- Gestion des réunions des instances représentatives du personnel : convocations, documents préparatoires, procès-verbaux

- **Outil informatique et téléphonie :** *suivi, maintenance et sécurisation du parc informatique, gestion des messageries électroniques, agendas et annuaires professionnels, etc..*
Gestion et maintenance du parc téléphonique, maîtrise des dépenses liées à l'utilisation des services de téléphonie, etc.

Nom, prénom, fonction, service, adresses professionnelles y compris électronique, numéro de ligne, numéro de téléphone appelé, service utilisé, opérateur appelé, nature de l'appel (sous la forme : local, départemental, national, international), durée, date et heure de début et de fin d'appel, éléments de facturation (nombre de taxes, volume et nature des données échangées à l'exclusion du contenu de celles-ci et coût du service utilisé).

Des données sensibles sont-elles traitées ?

[X] Oui [ ] Non

- Date et lieu de naissance
- Données relatives aux accidents du travail et maladies professionnelles ou maladies/pathologies non professionnelles pouvant avoir une incidence sur le poste.

Durées de conservation des catégories de données

Lors du recrutement :

Etat-civil, identité, données d'identification, images du candidat : 2 ans à compter du dernier contact avec le candidat.

En tant que salarié :

Etat-civil, identité, données d'identification, images des employés/ Gestion administrative / Organisation du travail / Action sociale et représentation du personnel : Le temps de la période d'emploi de la personne concernée (sauf dispositions législatives ou réglementaires contraires). Au-delà, ces données sont archivées sur un support informatique à accès très limité au RAF et la directrice, conformément aux règles applicables en matière d'archives publiques et d'archives privées.

Catégories de destinataires des données

Destinataires internes

1. Directrice, Responsable Administratif et Financier, Assistante de Direction ;
2. Le personnel ;
3. Instances représentatives du personnel : Comité Social Economique (CSE)
4. Instance de Gouvernance

Destinataires externes

1. Organismes gérant les différents systèmes d'assurances sociales, d'assurances chômage, de retraite et de prévoyance.
2. Organismes publics et administrations légalement habilités à recevoir les données ;
3. Organismes financiers intervenant dans la gestion des comptes de l'entreprise et du salarié.

Transferts des données hors UE

☐ Oui ☒ Non

Mesures de sécurité

☒ Contrôle d'accès des utilisateurs

Tous les documents papiers relatifs à la gestion du personnel sont stockés au siège social dans les bureaux des personnes habilitées à traiter des données concernant la gestion des ressources humaines.

☒ Mesures de traçabilité

Tous les documents informatisés relatifs à la gestion des ressources humaines sont stockés chez notre hébergeur extérieur PROGINOV. Seules les personnes habilitées à traiter des données concernant la gestion des ressources humaines peuvent y avoir accès via un mot de passe individuel.

☒ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Antivirus, mot de passe individuel.

[X] Sauvegarde des données

PROGINOV a choisi de stocker toutes les données sur des baies de stockage haute performance connectées en fibre optique. Un réseau de stockage dédié aux clients santé a été créé et l'utilisation d'unité de stockage logique par client permet l'étanchéité totale entre eux.
Les baies de stockage sont systématiquement doublées. Les données sont dupliquées en temps réel
Un « cluster » (groupe de serveurs) de Serveurs de sauvegarde pilote une bandothèque pour la gestion centralisée des sauvegardes.

Le cycle de Sauvegarde est quotidien :

- Bureautique et Messagerie : incrémentale quotidienne sur 20 jours + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort
- Base de données : incrémentale quotidienne sur 31 jours et complète 27 quinzaines + une copie externalisée des locaux de PROGINOV et stockée dans un coffre-fort

[x] Chiffrement des données

Les données transitant sur le réseau entre les postes de travail et les serveurs sont cryptées (cryptage SSL)

[X] Autres mesures :

- Signature d'un engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel ou sensible.
- Autorisation individuelle (signature) à utiliser la photographie dans le cadre d'un objectif précis.
- Autorisation individuelle à contacter "les personnes à prévenir en cas d'urgence" (cf Fiche Salarié)
- Fiche de poste co-signée
- Information "Traitement des données personnelles –Gestion du personnel et paye"
- Information du candidat à l'embauche sur le traitement des données personnelles
- Destructeur interne de documents dans chaque centre.

PROGINOV dispose depuis le 3 novembre 2014, de l'agrément par le Ministère des affaires sociales, de la santé et des droits des femmes, conformément au décret n°2006-6 du 4 janvier 2006, en tant qu'hébergeur de données de santé à caractère personnel. Cet agrément vaut pour toute « prestation d'hébergement de données de santé à caractère personnel collectées au moyen d'applications fournies par les clients à des fins de suivi médical ».
Par ailleurs PROGINOV a engagé une démarche visant à la conformité à la norme ISO 27001 et au code des bonnes pratiques préconisées par la norme ISO 27002.
L'ensemble des mesures prises en vue de la protection d'accès, l'intégrité aux données et la sauvegarde des données sont décrits dans un document intitulé « Santé annexe 2 : présentation du service d'Hébergement »

Protection d'accès au Système d'Information du Service de Santé au Travail

- Protection et intégrité physique

Le Système d'Information est dupliqué en temps réel, dans 2 « Datacenters » indépendants aussi bien en termes d'alimentation électrique, de climatisation, que de lignes de communications situées au 36 Rue de la Guillauderie 44118 LA CHEVROLIERE et au 2 rue Gustave Eiffel 44118 LA CHEVROLIERE. La continuité de service est assurée par la redondance de l'ensemble des équipements et services.

Les locaux de PROGINOV sont sécurisés sur le périmètre par un grillage autour de l'ensemble du terrain, un contrôle par barrière infrarouge relié au système d'alarme et au PC de surveillance.

Le contrôle d'accès aux locaux se fait par un système de badge individuel qui contrôle et enregistre les accès des personnes (horaires autorisés ou non, types de locaux autorisés ou non). L'extérieur des locaux est filmé en vidéosurveillance 24h/24 et 7jrs/7. Les images sont conservées jusqu'à 30 jours.

Activité 7 : L'accès aux locaux

Date de création de la fiche	**07 septembre 2018**
Date de dernière mise à jour de la fiche	**6 juin 2023**
Nom du logiciel ou de l'application	

Objectifs poursuivis

- Contrôle des accès aux locaux du siège et centres annexes de l'entreprise afin d'assurer la sécurité des biens.

Catégories de personnes concernées

1. Employés de l'entreprise
2. Prestataire de service : société de nettoyage

Catégories de données collectées

Listez les différentes données traitées

[X] **identité, numéros de badges**

Des données sensibles sont-elles traitées ?

[ ] Oui [X] Non

Durées de conservation des catégories de données

Jusqu' au départ du salarié de l'entreprise.

Catégories de destinataires des données

Destinataires internes

1. Personnels habilités dans le cadre de leurs fonctions, Responsable Administratif et Financier, Directrice, Assistante de direction

Sous-traitants

1. Prestataire de service : société de nettoyage

Transferts des données hors UE

[ ] Oui [X] Non

Mesures de sécurité

[X] Contrôle d'accès des utilisateurs

- Alarme anti-intrusion au siège.
- Au siège : verrouillage automatique des portes magnétiques – accès par badges en dehors des horaires d'ouverture

- Clés (centres annexes).
- Engagement individuel de réception et restitution des badges et clés (stockés dans les dossiers individuels des salariés, dans le bureau de l'Assistante de direction)

[X] Mesures de traçabilité

Le fichier Excel décrivant les utilisateurs de badges est sur le l'ordinateur du Responsable Administratif et Financier. Celui-ci est protégé par un mot de passe lors de l'ouverture de l'ordinateur. Il se trouve sous le répertoire Z:\\stephane\Badges locaux Bourg.

[ ] Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

[X] Sauvegarde des données

Le fichier Excel décrivant les utilisateurs de badges est sauvegardé tous les jours chez PROGINOV.

[ ] Chiffrement des données

[X] Contrôle des sous-traitants

Formulaire co-signé de remise de clés voire autres moyens d'accès aux locaux, à la société de nettoyage, pour tous les centres fixes. Il est classé dans l'armoire de l'Assistante de direction.

[X] Autres mesures :

Signature d'un engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel ou sensible.