RGPD

Sécurité informatique et sécurité de l'information

Politique de l'institution quant à la sécurité des données personnelles

---

L'institution collecte et traite des données personnelles dans les domaines suivants (à adapter et compléter selon votre situation) :

- Bénéficiaires MAE :
  La finalité du traitement est de garantir l'accueil optimal de l'enfant, sur le plan éducatif, social, sanitaire et financier.
  Les données récoltées sont classifiées comme suit :
  - Données inscription enfant ;
  - Données présence enfant ;
  - Données intervention accueil des parents ;
  - Données du carnet de l'enfant ;
  - Données de santé ????
- Travailleurs salariés de l'institution :
  La finalité du traitement est la gestion sociale et fiscale de travailleurs salariés dont la responsabilité finale incombe à l'employeur.
  Les données récoltées sont classifiées comme suit :
  - Données de sélection et recrutement ;
  - Données d'identité ;
  - Données administratives ;
  - Données juridiques ;
  - Données d'équipement de protection individuelle ;
- Membres et administrateurs de l'institution :
  La finalité du traitement est le respect de la législation relative aux asbl et des obligations d'identification des membres et des administrateurs.
  Les données récoltées sont classifiées comme suit :
  - Données d'identité ;
  - Données de contact et de compétence ;
- Fournisseurs :
  La finalité du traitement est de disposer des éventuelles données personnelles du contact le plus approprié chez le fournisseur en fonction de la demande.
  Les données récoltées sont classifiées comme suit :
  - Données d'identité ;
- Partenaires :
  La finalité du traitement est de disposer des éventuelles données personnelles du contact le plus approprié chez le partenaire en fonction de la demande.
  Les données récoltées sont classifiées comme suit :
  - Données d'identité ;

Ces données personnelles ne sont jamais vendues à des tiers, pour quelque raison que ce soit.

Toute personne concernée par la récolte et le traitement de certaines de ces données personnelles peut prendre contact avec la direction de l'institution afin que celle-ci, en fonction de la demande, oriente la personne auprès du service compétent.
Les coordonnées de la direction sont les suivantes :
……..

Vous trouverez également dans ce document la politique de l'institution en matière de sécurité informatique et de sécurité de l'information.

Pour l'élaboration de ce guide relatif à la sécurité des données personnelles, l'institution a veillé à élaborer, pour chaque registre de traitement de données à caractère personnel, une gestion des risques comprenant les éléments suivants :

- L'identification des impacts potentiels sur les droits et libertés des personnes concernées si l'un des événements suivants survient :
    - L'accès illégitime aux données personnelles ;
    - La modification non désirée de données personnelles ;
    - La disparition de données personnelles ;
- L'identification des sources de risques (qui ou quoi pourrait être à l'origine de chaque événement redouté) ;
- L'identification des menaces réalisables (qu'est-ce qui pourrait permettre que chaque événement redouté survienne) ;
- La détermination des mesures existantes ou prévues qui permettent de traiter ces risques ;
- La gravité et la vraisemblance de ces risques.

De cette analyse de gestion des risques, l'institution a mis en place la politique de sécurité reprise ci-dessous.

En caractère « ordinaire », nous reprenons les éléments qui peuvent composer la politique de l'institution en matière de sécurité des données personnelles, document qui pourrait être remis aux personnes concernées par la collecte et le traitement de données personnelles sur simple demande.

En caractère italique, vous trouverez divers documents ou exemples qui peuvent être utilisés en interne.

Sensibilisation des collaborateurs

Dès leur engagement et tout au long de leur parcours professionnel au sein de l'institution, les collaborateurs sont sensibilisés à l'importance du devoir de discrétion et de réserve, voire de secret professionnel dans la connaissance, la collecte et l'utilisation de données personnelles.

C'est ainsi que l'institution s'est dotée des outils suivants :

- Une charte informatique ;
- Des clauses de confidentialité prévues pour certains contrats de travail.

Annexe A – Charte informatique

Tout travailleur de l'institution doit avoir conscience qu'il peut, à tout moment, disposer de données personnelles relatives à des personnes physiques.

Ceci concerne tant les bénéficiaires que les collègues, les membres du pouvoir organisateur, les fournisseurs, les partenaires,….

Le travailleur reconnait avoir eu, lors de son engagement et régulièrement lors de son occupation au sein de l'institution, des informations et formations, formelles et informelles, relatives à l'importance que tout collaborateur doit accorder à la protection de données privées et personnelles dont il peut disposer dans l'exercice de sa fonction.

Le travailleur a connaissance du fait que la politique de protection des données personnelles mise en place au sein de l'institution répond aux prescrits du Règlement (UE) 2016/679 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 (communément appelé RGPD pour Règlement Général de Protection des Données).

Le non respect de cette charte informatique peut entrainer l'application de sanctions envers le travailleur pouvant aller jusqu'à la rupture du contrat de travail si la gravité des actes ou omissions posés par le travailleur ont des conséquences importantes pour la personne concernée par la violation de ces données privées.

Toute question, remarque, suggestion, plainte doit être déposée par le travailleur auprès de …… (nom, titre et ou fonction et moyens de contact).

Protection des données à caractère personnel :

Toute personne ayant communiqué des données personnelles, y compris les travailleurs de l'institution pour leurs propres données, disposent des protections suivantes :

- *Droit d'accès et de rectification des données*

A tout moment, vous pouvez prendre contact avec …….. (nom, titre et ou fonction et moyens de contact) afin de connaître les données personnelles dont dispose l'institution, la façon dont ces données sont conservées. A ce droit d'accès est lié un droit de rectification s'il s'avère que ces données sont obsolètes.
La personne physique doit disposer des éléments lui permettant de prendre contact avec l'institution qui a récolté et conservé ses données personnelles pour y avoir accès et les rectifier si nécessaire.

- *Droit de portabilité*

Chaque travailleur a le droit, pour ce qui le concerne :
- *de recevoir ses propres données dans un format structuré, couramment utilisé et lisible par une machine (PC) ;*
- *et si c'est techniquement possible, d'obtenir que les données soient directement transmises à un autre responsable de traitement (ceci ne vise que les données dont le responsable de traitement dispose en raison du consentement écrit de la personne concernée et pour lesquelles le traitement est effectué à l'aide de procédés automatisés).*

- *Droit à l'effacement (ou droit à l'oubli numérique)*

La personne concernée a le droit d'obtenir l'effacement de ses données dans les meilleurs délais dans les cas suivants :
- *les données à caractère personnel ne sont plus nécessaires au regard des finalités poursuivies ;*

- *elle retire le consentement sur lequel est fondé le traitement ;*
- *elle s'oppose au traitement de ses données à des fins de prospection ;*
- *les données ont fait l'objet d'un traitement illicite ;*
- *les données ont été collectées dans le cadre de l'offre directe de service à un enfant de moins de 16 ans.*

Le droit à l'effacement ne concerne donc pas les données personnelles récoltées dans le cadre de la gestion sociale et fiscale des travailleurs salariés.

<u>Règles d'utilisation des outils informatiques :</u>

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle.

En interne, toute question d'ordre strictement informatique doit être adressée à ……(nom, titre et ou fonction et moyens de contact).

Le responsable informatique interne peut, conformément aux règles prévues par la CCT n° 81 conclue au sein du Conseil National du Travail le 26 avril 2002 et relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électronique en réseau, contrôler l'usage des TIC au sein de l'institution. Le travailleur veillera à se référer au contenu du règlement de travail en la matière.

Chaque travailleur dispose, à l'engagement, d'un mot de passe et log in personnels adaptés aux outils informatiques mis à sa disposition.

Le travailleur peut modifier ces mots de passe et log in moyennant l'accord préalable du responsable informatique et dans le respect des consignes qui lui seront données. Le responsable informatique et la direction doivent, en tout temps, disposer des mots de passe et log in actifs.

Par ailleurs, le travailleur s'engage à respecter les règles de sécurité suivantes :
- *signaler au responsable informatique interne toute violation ou tentative de violation suspectée de son compte réseau, et de manière générale tout dysfonctionnement ;*
- *ne jamais confier ses mot de passe et log in ;*
- *ne jamais demander ses mot de passe et log in à un collègue de travail ;*
- *ne pas masquer sa véritable identité ;*
- *ne pas usurper l'identité d'autrui ;*
- *ne pas modifier les paramétrages du poste de travail ;*
- *ne pas installer de logiciels sans l'autorisation préalable du responsable informatique interne ;*
- *ne pas copier, modifier, détruire les logiciels appartenant à l'institution ;*
- *verrouiller son ordinateur dès qu'il quitte son poste de travail ;*
- *ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas ;*
- *ne pas copier de données sur un support externe (clé USB, smartphone, disque dur externe,….) sans l'accord préalable du responsable informatique interne.*

En ce qui concerne les personnes externes à l'institution (stagiaires, étudiants, partenaires sous-traitants,…), ils ne peuvent avoir accès aux outils informatiques sans l'accord préalable du responsable informatique interne.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte informatique par leurs travailleurs salariés.

<u>Les outils informatiques :</u>

- *Poste de travail fixe*

L'institution met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions.

Le travailleur ne doit pas :

- *Modifier ces équipements et leur fonctionnement, leur paramétrage ainsi que leur configuration physique ou logicielle ;*
- *Connecter ou déconnecter du réseau des outils informatiques et de communication sans y avoir été autorisé par le responsable informatique interne ;*
- *Déplacer l'équipement informatique ;*
- *Nuire, volontairement ou non, au fonctionnement des outils informatiques et de communications.*

Toute installation de logiciels supplémentaires est subordonnée à l'accord du responsable informatique interne.

- *Equipements nomades (PC portable, smartphone, clé USB,….)*

L'utilisateur veillera à en avoir l'utilisation balisée par le responsable informatique interne :

- *Quant au contenu se trouvant dans ces équipements (autant que faire se peut, les équipements mobiles ne comprennent pas de données personnelles) ;*
- *Quant aux modalités d'utilisation :*
  - *Verrouillage ;*
  - *Mot de passe et log in ;*
  - *Signalisation immédiate d'une perte ou d'un vol ;*
  - *Utilisation strictement professionnelle ;*
  - *Pas de prêt à un membre de la famille ou à tout tiers ;*
  - *….*

- *Messagerie électronique*

La messagerie mise à la disposition du travailleur est destinée à un usage professionnel.

L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail du travailleur concerné ni la sécurité du réseau informatique. A voir si ce point n'est pas en contradiction avec votre règlement de travail

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

L'institution s'interdit d'accéder aux dossiers et aux messages identifiés comme « personnel » dans l'objet de la messagerie du travailleur.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par le responsable informatique interne et validées par la direction de l'institution :

- *Volumétrie de la messagerie ;*
- *Taille maximale de l'envoi et de la réception d'un message ;*
- *Nombre limité de destinataires simultanés lors de l'envoi d'un message ;*
- *Gestion de l'archivage de l messagerie ;*
- *….*

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur support externes.

Les travailleurs peuvent consulter leur messagerie à distance, à l'aide d'un navigateur (webmail). Les fichiers qui seraient copiés sur l'ordinateur utilisé par le travailleur dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé. On peut aussi prévoir que ce mode de travail est interdit

En cas d'absence de courte durée du travailleur et afin de ne pas interrompre le fonctionnement du service, le responsable informatique interne peut ponctuellement transmettre au supérieur hiérarchique du travailleur un courriel à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur.

En cas d'absence de longue durée, le supérieur hiérarchique peut demander au responsable informatique interne, après accord de la direction, le transfert des messages reçus.

Par ailleurs, l'institution dispose d'un outil permettant de lutter contre la propagation de messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, le travailleur est invité à limiter son consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion, notamment si elles ne relèvent pas du cadre strictement professionnel.

- *Téléphonie*

L'institution met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et/ou mobiles.

L'utilisation du téléphone à titre privé est interdite sauf si le travailleur se voit comptabiliser un avantage de toute nature dans ce cadre.

En cas d'utilisation à titre strictement professionnel, et conformément aux instructions établies par l'ONSS, l'employeur se réserve le droit de vérifier, par le biais des factures de l'opérateur de téléphonie, que le caractère strictement professionnel des appels est respecté.

<u>L'administration du système d'information :</u>

A titre préventif, l'institution peut mettre en place des systèmes automatiques de filtrage permettant de diminuer les flux d'informations et d'assurer la sécurité et la confidentialité des données. Il peut s'agir du filtrage des sites internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (messagerie instantanée,….).

Le responsable informatique interne ou le sous traitant gérant l'informatique au sein de l'institution peut opérer sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril le fonctionnement ou l'intégrité du réseau informatique.
Pour ce faire, le service compétent s'appuie sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'événement.
Le service informatique est le seul utilisateur de ces informations qui sont effacées à l'expiration d'un délai de …. (par exemple 3 mois).

A des fins de maintenance informatique, le responsable informatique interne ou un sous traitant peut accéder à distance à l'ensemble des postes de travail. Si le travailleur est présent, il en sera prévenu à l'avance.

Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service informatique interne ou externe peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

<u>Procédure applicable lors du départ de l'utilisateur :</u>

Lors de son départ, le travailleur doit restituer au responsable informatique interne les matériels mis à sa disposition.

Il doit préalablement effacer ses fichiers et données personnelles. Toute copie de documents professionnels est strictement interdite.

Les mot de passe et log in de l'utilisateur sont supprimés dans les deux jours ouvrables.

Le travailleur reconnait avoir reçu ce ……./…./…. la charte informatique à jour au ……..

Signature du travailleur
(précédée de la mention
« lu et approuvé »)

Annexe B – Clause de confidentialité à annexer au contrat de travail

Exemple de clause de respect de la vie privée générale :

Les données personnelles du travailleur sont traitées par l'employeur dans le respect du Règlement (UE) 2016/679 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 (communément appelé RGPD pour Règlement Général de Protection des Données).

Exemple de clause de confidentialité pour le service administratif et/ou GRH :

La gestion des salaires des travailleurs de l'institution vous donne accès à des données confidentielles à caractère personnel.
Celles-ci doivent être gérées dans le strict respect du Règlement Général 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 (règlement UE 2016/679 du 27 avril 2016).
Vous vous engagez donc à ne pas utiliser, directement ou indirectement, les données dont vous avez connaissance en dehors du cadre strict de votre travail.
Cette clause de confidentialité vaut, tant au cours de l'exécution du contrat de travail qu'après la fin des relations contractuelles.
La divulgation, oralement ou par écrit, à des collègues ou à des tiers de données à caractère personnel, telles que la situation familiale, les données de prestation ou salariales, et ce en dehors du cadre professionnel, est constitutif d'un motif grave.

Exemple de clause de confidentialité pour le service de comptabilité :

Votre fonction au sein du service comptabilité vous donne accès à des données confidentielles à caractère personnel.
Ces données confidentielles peuvent concerner tant le personnel salarié de l'entreprise que les bénéficiaires du service, les prestataires indépendants, les fournisseurs, les administrateurs,…
Le croisement des données disponibles dans les divers logiciels utilisés par l'institution vous permet en effet de disposer d'une vue complète et détaillée tant de la structure financière de l'entreprise que de la situation sociale, fiscale et familiale de toutes les personnes qui gravitent autour de l'institution.
L'ensemble de ces données personnelles et confidentielles doit être géré dans le strict respect du Règlement Général 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 (règlement UE 2016/679 du 27 avril 2016).
Quant aux données financières de l'asbl, seules celles faisant l'objet d'une publication à la Banque Nationale de Belgique peuvent faire l'objet d'une diffusion interne ou externe à l'entreprise, avec information préalable auprès de la Direction.
De par votre fonction et les règles déontologiques y liées, vous vous engagez donc à ne pas utiliser, directement ou indirectement, les données dont vous avez connaissance en dehors du cadre strict de votre travail.
Cette clause de confidentialité vaut, tant au cours de l'exécution du contrat de travail qu'après la fin des relations contractuelles.
La divulgation à des collègues ou à des tiers de données à caractère personnel ou à caractère financier, telles que la situation familiale, les données de prestation ou salariales, la situation des comptes de l'asbl,…,et ce en dehors du cadre professionnel, est constitutif d'un motif grave.

Exemple de clause de confidentialité largement inspiré du modèle de la CNIL

Je soussigné/e Monsieur/Madame _____, exerçant les fonctions de _____ au sein de la société _____
(ci-après dénommée « la Société »), étant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.
Je m'engage par conséquent, conformément aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.
Je m'engage en particulier à :

- *ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;*
- *ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;*
- *ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;*
- *prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;*
- *prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;*
- *m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;*
- *en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.*

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.
J'ai été informé que toute violation du présent engagement m'expose à des sanctions pouvant aller jusqu'à la rupture du contrat de travail

Annexe C – Directives relatives à l'utilisation du courriel et d'internet à annexer au règlement de travail

ANNEXE … AU REGLEMENT DE TRAVAIL
DIRECTIVES RELATIVES A L'UTILISATION DU COURRIER ELECTRONIQUE ET D'INTERNET AU SEIN DE L'INSTITUTION

Préambule

L'employeur fournit à ses travailleurs un accès à l'internet et un compte Email en vue de faciliter la communication au sein de l'entreprise et avec les tiers. Cet outil de travail ne peut être utilisé qu'à des fins professionnelles.

1. Objet et portée de la directive

Cette annexe définit la position de l'employeur à propos :

- *de l'utilisation du courrier électronique (e-mail) ;*
- *de l'accès à l'internet (sites www, forums de discussion, etc.) ;*
- *de la surveillance du système de courrier électronique et d'accès à internet et du respect de la vie privée du travailleur.*

Les présentes instructions sont applicables à l'ensemble des travailleurs. Leur violation peut donner lieu à l'application des sanctions définies dans le règlement de travail.

2. Responsabilités

Chaque travailleur est responsable de l'usage du système informatique mis à sa disposition conformément aux présentes instructions.
Pour des raisons liées à la sécurité et au bon fonctionnement du réseau informatique de l'institution dans le respect du RGPD, la ou les personnes responsables du service informatique a le droit de surveiller quand bon lui semble toute activité effectuée par le biais du système informatique de l'entreprise, en ce compris les activités relatives à l'usage de l'e-mail et d'internet, dans le respect des dispositions légales applicables.
La ou les personnes responsables du service informatique ont le pouvoir de rechercher et de rapporter à la direction toute infraction aux présentes instructions.

3. Instructions

3.1. Activités prohibées

Sont strictement interdits :

- *la diffusion d'informations confidentielles relatives à l'employeur, aux travailleurs, aux partenaires et aux bénéficiaires en dehors du cadre professionnel ;*
- *la diffusion ou le téléchargement de données protégées par le droit de la propriété intellectuelle ;*
- *la participation à une activité professionnelle annexe ;*
- *le « forwardind » de messages électroniques en l'absence de but professionnel légitime, dans des circonstances de nature à porter préjudice à l'auteur du message originel ;*
- *l'envoi de messages ou la consultation de sites dont le contenu est susceptible de porter atteinte à la dignité d'autrui, notamment l'envoi de messages ou la consultation de sites racistes, révisionnistes, prônant la discrimination sur base du sexe, de l'orientation sexuelle, du handicap, de la religion ou des convictions religieuses d'une personne ou d'un groupe de personnes ;*
- *l'envoi et (ou), en cas de réception, l'ouverture de fichiers « exécutables », en raison de la menace sérieuse qu'ils constituent pour la stabilité et la sécurité du réseau de l'employeur (virus, etc.) ;*
- *la consultation de sites à caractère érotique ou pornographique ;*
- *l'utilisation de l'e-mail et de l'internet dans le cadre d'une activité (professionnelle ou non) étrangère au contrat de travail liant l'employé à l'employeur ;*
- *la participation à des « chaînes de lettres » ;*
- *plus généralement, l'utilisation de la messagerie électronique ou de l'internet dans le cadre*

d'une activité illégale, quelle qu'elle soit ainsi qu'en vue d'un usage à caractère privé.
Cette énumération n'est pas limitative.

3.2. Utilisation du courrier électronique

La destination exclusive du système de courrier électronique, comme celle de tout système informatique de l'institution, est exclusivement professionnelle.
Exceptionnellement, l'employeur tolère, sans autorisation préalable, ***l'usage exceptionnel*** *à des fins privées du système de messagerie électronique, à condition que cet usage soit* ***occasionnel,*** *se déroule en dehors du temps de travail, n'entrave en rien la réalisation du travail du travailleur ni le bon fonctionnement de l'institution et qu'il ne constitue pas une infraction aux présentes instructions, aux dispositions légales, au contrat de travail ou au règlement de travail.*
S'il fait usage de cette faculté, le travailleur est tenu d'indiquer, dans le sujet du message, que celui-ci a un caractère privé en précisant dans l'objet du message la mention « courrier personnel ». Il doit en outre supprimer, dans le corps du message, toute mention relative à l'employeur (telle que la signature automatique) et toute autre indication qui pourrait laisser croire que le message est rédigé par le travailleur dans le cadre de l'exercice de ses fonctions. Par ailleurs, le travailleur s'efforcera d'appliquer les mesures de prudence et de sécurité d'usage quant aux pièces jointes.
Le travailleur ne transmet son adresse e-mail professionnelle qu'en vue de recevoir des messages professionnels. S'il advient que des courriers à titre privé lui soient envoyés sur son adresse e-mail professionnelle, il informe d'initiative son correspondant de lui adresser le courrier personnel à son adresse e-mail personnelle.

3.3. Utilisation d'internet

L'employeur fournit à ses travailleurs l'accès à internet à des fins exclusivement professionnelles. Il n'assume aucune responsabilité à l'égard de ses travailleurs en ce qui concerne le contenu des sites visités.

Lorsqu'ils parcourent l'internet, les travailleurs doivent respecter les règles suivantes :

- *l'accès à Internet ne peut être utilisé aux fins prohibées au point 3.1 ;*
- *l'utilisation d'Internet ne peut se faire qu'à des fins professionnelles. L'exploration d'Internet dans une optique d'apprentissage et de développement personnel est acceptée mais ne peut en rien porter atteinte au bon fonctionnement du réseau ou détourner le travailleur du travail qu'il doit réaliser. Elle se fera en principe exclusivement durant les temps de pause ;*
- *l'employeur se réserve le droit de bloquer à tout moment et sans avertissement préalable l'accès aux sites dont il juge le contenu illégal, offensant ou inapproprié ;*
- *l'attention des travailleurs est attirée sur le fait que la plupart des sites Internet qu'ils visitent gardent une trace de leur passage. Dans certains cas, ces sites identifient précisément la provenance du visiteur et son identité électronique (en l'occurrence celle de l'employeur).*

4. Surveillance de la messagerie électronique et de l'internet par l'employeur

4.1. Le principe général

L'employeur peut exercer un contrôle de l'usage de l'e-mail et d'internet dans le respect des dispositions légales applicables, notamment la loi du 8 décembre 1992, le Règlement Général pour la Protection des Donnés du 27 avril 2016 et la C.C.T. n° 81 du 26 avril 2002. Il est rappelé que toute information circulant et (ou) stockée sur les systèmes informatiques de l'institution est considérée comme ayant un caractère professionnel et est toujours censée être mise à la disposition de l'employeur par le travailleur. Le travailleur qui souhaite faire usage de la faculté d'utiliser, à titre exceptionnel, la messagerie électronique à des fins privées est tenu d'indiquer clairement dans le sujet du message, que celui-ci a un caractère privé, conformément à l'article 3.2. ci-dessus.

Le contrôle poursuit notamment les finalités suivantes :

1. *la prévention et la répression de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ainsi que la répression de ces faits ;*
2. *la protection des intérêts de l'institution ;*
3. *la sécurité et (ou) le bon fonctionnement technique des systèmes informatiques en réseau, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de*

l'entreprise ;

4. *le respect de bonne foi des principes et règles d'utilisation des technologies en réseau, de l'e-mail et d'internet tels que définis dans cette annexe.*

L'employeur respecte le principe de proportionnalité dans la poursuite de ces finalités.

4.2. Le contrôle de l'utilisation d'internet

L'employeur maintient automatiquement une liste générale des sites internet consultés via le réseau de l'institution, indiquant la durée et le moment des visites. Cette liste ne fait pas directement mention de l'identité du travailleur. Elle est régulièrement évaluée par l'employeur.
Lorsque, à l'occasion de ce contrôle général ou au départ d'autres sources d'information, l'employeur constate une anomalie, il se réserve le droit, dans le cadre de la poursuite des finalités décrites au point 4.1., de procéder à l'identification d'un travailleur, conformément à la procédure d'individualisation décrite au point 4.4. ci-après.

4.3. Le contrôle du courrier électronique

Sur base d'indices généraux tels la fréquence, le nombre, la taille, les annexes, etc. des messages électroniques, certaines mesures de contrôle pourront être prises par l'employeur vis-à-vis de ces messages, dans le cadre de la poursuite des finalités décrites au point 4.1. ci-dessus.
Si l'employeur présume un usage anormal ou interdit du système de courrier électronique, il procédera, dans le cadre de la poursuite des finalités décrites au point 4.1. ci-dessus, à l'identification du travailleur concerné dans le respect de la procédure d'individualisation décrite au point 4.4. ci-dessous.

4.4. Les mesures d'individualisation

Par « individualisation », on entend le traitement des données collectées lors d'un contrôle en vue de les attribuer à un travailleur identifié ou identifiable.

Individualisation directe

L'employeur peut procéder à une individualisation directe s'il suspecte ou a constaté :

- *la commission de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;*
- *la communication de données confidentielles ;*
- *une menace à la sécurité et (ou) au bon fonctionnement technique des systèmes informatiques en réseau de l'institution.*

Individualisation indirecte

Si l'employeur constate un manquement aux présentes directives, autres que celles décrites plus haut, l'employeur avertira l'ensemble des travailleurs par le biais du courrier électronique. En cas de récidive endéans les trois mois, l'employeur identifiera le travailleur qui s'en est rendu coupable.

Le travailleur qui a enfreint les présentes directives peut être sanctionné et le comportement fautif peut entraîner la rupture du contrat voire un licenciement pour motif grave si la faute est considérée comme grave.

4.5. Les questions et les plaintes

Chaque travailleur peut s'adresser à .....pour toute question concernant l'application de ces instructions.
Cette personne traite également les plaintes concernant l'usage d'internet ou du courrier électronique au sein de l'institution. Les travailleurs qui s'estiment victimes d'actes prohibés par les présentes directives peuvent s'adresser à cette personne.

Chaque travailleur peut contacter la direction au ou à l'adresse électronique suivante : pour des questions techniques concernant l'utilisation d'internet et du courrier électronique.

Conformément à la politique de sécurité de l'information et informatique de l'institution, le travailleur dispose des droits suivants :

- *droit d'accès et de rectification de ses données personnelles ;*
- *droit de portabilité ;*
- *droit à l'effacement (ou droit à l'oubli numérique).*

Authentification des utilisateurs

Option pour les institutions fonctionnant en réseau

Pour s'assurer que chaque utilisateur accède uniquement aux données dont il a besoin, l'institution dote chaque travailleur d'un identifiant qui lui est propre et veille à ce qu'il doive s'authentifier avant toute utilisation des moyens informatiques (mot de passe et log in).

Le travailleur chargé de la gestion informatique de la structure et la direction disposent des mots de passe et log in de l'ensemble du personnel. Le stockage des authentifiants s'effectue de façon sécurisée.

De préférence, l'authentifiant reprend 12 caractères minimum et 4 types de caractères (majuscule, minuscule, chiffre, caractère spécial).

Il est conseillé de prévoir un verrouillage du compte après « x » échecs.

Si l'authentifiant est attribué par un administrateur ou automatiquement par le système lors de la création du compte ou lors d'un renouvellement consécutif à un oubli, il est conseillé d'obliger l'utilisateur à modifier cet authentifiant dès sa première connexion.

Il est également conseillé d'imposer un renouvellement de l'authentifiant selon une périodicité « pertinente et raisonnable ».

Pour le stockage de mots de passe de façon sécurisée, il est conseillé, au minimum, d'utiliser une fonction de hachage cryptographique utilisant un sel (aléa utilisé lorsqu'il est différent pour chaque mot de passe stocké) ou une clé (l'aléa utilisé est commun à la transformation d'un ensemble de mots de passe). A voir avec le service informatique.

Option pour les institutions ne fonctionnant pas en réseau

Chaque ordinateur est indépendant et chaque travailleur dispose de son code accès spécifique, créé par lui-même.

Il y a un ordinateur par poste de travail et dédié à un seul travailleur.

Il s'agit de PC fixes et non de portables et aucun accès aux données n'est prévu via internet.

Afin de garantir la continuité du service en cas d'absence d'un travailleur, chaque travailleur communique au responsable informatique ses codes d'accès à chaque modification de ceux-ci. La gestion des ordinateurs et la consultation des fichiers se fait en conformité avec la CCT n° 81 faisant partie intégrante du règlement de travail.

Gestion des habilitations

_____

Option pour les institutions fonctionnant en réseau

Chaque travailleur disposant d'un mot de passe et log in personnel n'a accès qu'aux seules données strictement nécessaires à l'accomplissement de ses missions.

Les éventuels stagiaires et étudiants effectuant un stage au sein de l'institution disposent, si le contenu du stage le justifie, d'un mot de passe et log in personnel limité à la durée de leur stage ou contrat.

En cas de suspension du contrat de travail, les mots de passe et log in sont bloqués.

En cas de fin du contrat de travail, les mots de passe et log in sont désactivés endéans les 24 heures.

Par ailleurs, chaque début d'année civile, une revue annuelle des habilitations est réalisée afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.

Toute information complémentaire relative à cette gestion des accès peut être obtenue auprès de ……..

Option pour les institutions ne fonctionnant pas en réseau

Chaque travailleur communique au responsable informatique ses codes d'accès à chaque modification de ceux-ci. La gestion des ordinateurs et la consultation des fichiers se fait en conformité avec la CCT n° 81 faisant partie intégrante du règlement de travail.

En cas d'oubli de ses codes d'accès, le travailleur s'adressera au responsable informatique. Celui-ci veillera à ce que les codes d'accès répondent aux prescriptions minimales de sécurité informatique.

Traçage des accès et gestion des incidents

<u>Option pour les institutions fonctionnant en réseau</u>

L'institution a mis en place une procédure afin de pouvoir identifier un accès frauduleux, une utilisation abusive de données personnelles ou de déterminer l'origine d'un incident.

Cette procédure consiste en un système de journalisation (appelé « log ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité informatique.

Cette journalisation concerne les accès des utilisateurs en incluant leur identifiant, la date et l'heure de la connexion, la date et l'heure de la déconnexion.

Les équipements de journalisation et les informations journalisées sont conservés et protégés par la personne responsable de la sécurité informatique. Celle-ci est la seule à avoir accès à ces données. Elle en gère l'utilisation conformément au RGPD et à la CCT n° 81 du Conseil National du Travail. Le responsable de la sécurité informe le responsable de traitement de toute anomalie ou incident de sécurité informatique.

Ces journaux sont conservés durant une période de 12 mois. Délai à fixer.

Sécurisation des postes de travail

Système antivirus, antispam, pare-feu et autre protection contre l'extérieur

Option pour les institutions fonctionnant avec un sous-traitant

L'institution a recours aux compétences techniques et informatiques d'un sous-traitant.

Celui-ci veille à protéger le système informatique de l'institution des intrusions externes en veillant à ce que le système réseau et/ou les ordinateurs bénéficient d'une protection optimale et mise à jour, en recourant aux systèmes les plus fiables se trouvant sur le marché.

Option pour les institutions ne fonctionnant pas avec un sous-traitant

L'institution se dote des protections les plus fiables présentes sur le marché. Elle veille à mettre à jour régulièrement ces systèmes de protection en se documentant périodiquement quant aux nouveautés en la matière.

Back up

Option pour les institutions fonctionnant en réseau

Un back up de toutes les données se trouvant sur le réseau est effectué tous les …… jours.

La personne chargée de la sécurité informatique vérifie régulièrement que les back up sont effectués correctement et que le contenu est lisible.

Le back up est sauvegardé à l'extérieur de l'institution OU un second back up est sauvegardé, via un sous-traitant, dans un cloud à l'extérieur de l'institution.

Option pour les institutions ne fonctionnant pas en réseau

Un back up est réalisé par le responsable de la sécurité informatique ou une personne déléguée tous les …. Jours pour chaque ordinateur, fixe ou portable, de l'institution.

Chaque travailleur veillera à se conformer aux instructions données par le responsable informatique pour que ce back up se réalise à temps et à heure.

CE back up est sauvegardé en un endroit extérieur à l'institution.

Autres mesures

La connexion de supports mobiles (clé USB, disque dur externe,…) n'est autorisée qu'avec l'accord préalable du responsable de la sécurité informatique. Il en va de même pour l'exécution d'applications téléchargées.

L'institution veille à effacer, de façon sécurisée, les données présentes sur un poste de travail préalablement à sa réaffectation à une autre personne.

Sécurisation de l'informatique mobile

Seuls les moyens informatiques mobiles mis à disposition par l'institution peuvent être utilisés à des fins professionnelles.

Pour chaque type d'outil (PC portable, clé USB, smartphone,…), des mesures de sécurité en termes d'accès au contenu (type verrouillage et déverrouillage) sont prévues par le responsable de la sécurité informatique.

Le responsable de la sécurité informatique dispose d'une liste des outils informatiques mobiles, en lien avec les utilisateurs, les mots de passe et log in. Il vérifie, de façon régulière, qu'aucune perte ou vol ne doit être déploré.

La reprise de ces outils informatiques mobiles, voire leur blocage est géré par le responsable de la sécurité informatique.

Protection du réseau informatique interne

Ce point doit être rédigé en lien avec les informations techniques communiquées par votre service informatique.

Vous trouverez ci-dessous quelques éléments communiqués par la CNIL (pendant français de l'Autorité de Protection des Données, anciennement Commission de Protection de la Vie Privée).

Les précautions élémentaires suivantes sont préconisées par la CNIL :

- Limiter les accès Internet en bloquant les services non nécessaires (VoIP, pair à pair, etc.) ;
- Gérer les réseaux Wi-Fi. Ils doivent utiliser un chiffrement à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe) et les réseaux ouverts aux invités doivent être séparés du réseau interne ;
- Imposer un VPN pour l'accès à distance ainsi que, si possible, une authentification forte de l'utilisateur (carte à puce, boitier générateur de mots de passe à usage unique (OTP), etc.) ;
- S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet. La télémaintenance doit s'effectuer à travers un VPN ;
- Limiter les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports.

Sécurisation des serveurs

La sécurisation des serveurs est réservée au service informatique qui dispose d'un accès dit « administrateur ».

Les opérations d'administration des serveurs s'effectuent via un réseau dédié et isolé, accessible après une authentification forte et avec une traçabilité renforcée.

L'institution dispose de systèmes de détection et prévention d'attaques spécifiques.

L'institution dispose de serveurs dits miroirs et réalisent également des back up journaliers conservés, soit dans un endroit ignifuge et étanche, soit dans un lieu externe au siège sociale de l'institution. Le service informatique effectue un suivi régulier de ces back up.

Ces serveurs se trouvent dans un endroit sécurisé.

Sécurisation du site internet

Ce point doit être rédigé en lien avec les informations techniques communiquées par votre service informatique.

Vous trouverez ci-dessous quelques éléments communiqués par la CNIL (pendant français de l'Autorité de Protection des Données, anciennement Commission de Protection de la Vie Privée).

Les précautions élémentaires suivantes sont préconisées par la CNIL :

- Mettre en œuvre le protocole TLS (en remplacement de SSL) sur tous les sites web, en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre ;
- Rendre l'utilisation de TLS obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques ;
- Limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées. Si l'accès à un serveur web passe uniquement par HTTPS, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port 443 et bloquer tous les autres ports ;
- Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées. En particulier, limiter l'utilisation des comptes administrateurs aux équipes en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent ;
- Si des *cookies* non nécessaires au service sont utilisés, recueillir le consentement de l'internaute après information de celui-ci et avant le dépôt du *cookie* ;
- Limiter le nombre de composants mis en œuvre, en effectuer une veille et les mettre à jour.

Sauvegarde et prévention de la continuité d'activité

Le responsable du service informatique dispose de la procédure à mettre en place en cas de disparition non désirée de données informatiques.

Le back up journalier des données du serveur permet une remise en route de l'ensemble des activités de l'institution endéans les 24 heures.

Le responsable de la sécurité informatique ou une personne déléguée teste régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprise de l'activité.

Exemple de plan de continuité d'activité ou de reprise d'activité

A rédiger avec le service informatique

Archivage de manière sécurisée

Si l'institution ne procède pas à un archivage

A ce jour, aucun archivage n'est réalisé, et ce pour les raisons suivantes :

- Le coût de l'archivage est disproportionné par rapport aux données privées récoltées ;
- Les données récoltées sont indispensables tout au long de la relation contractuelle avec les personnes visées et ne peuvent donc être archivées tant que la relation contractuelle perdure ;
- Les données récoltées sont par ailleurs nécessaires dans le cadre d'un contrôle du travail effectué par l'institution et/ou des subventions octroyées à l'institution et doivent donc rester disponibles tant que la prescription n'est pas atteinte.

Si l'institution procède à un archivage

Dans le cadre de la mise en réseau des données, les données personnelles non nécessaires à l'exécution des missions de l'institution ne sont plus accessibles au personnel de l'institution.

Un archivage est effectué une fois par année civile. Cet archivage est conservé durant 10 ans débutant le 1er janvier de l'année suivant ledit archivage ou un délai plus long si certaines données archivées doivent être conservées en raison d'une action en justice (délai de prescription).

Le serveur sur lequel sont stockées les données archivées bénéficient des mêmes protection et mesures de sécurité informatique que les autres serveurs de l'institution.

L'accès aux données archivées ne peut s'effectuer que moyennant l'accord préalable du responsable du service informatique et du responsable du traitement des données.

Les archives sont détruites par une société agréée à cette fin.

Encadrement de la maintenance et de la destruction des données

---

Les interventions de maintenance confiées à un sous-traitant sont prévues dans le respect d'une clause de sécurité et de confidentialité, sous la responsabilité du service informatique de l'institution et du responsable de traitement.

La convention avec ce sous-traitant prévoit également la destruction des données auxquelles le sous-traitant a éventuellement eu accès pour sa maintenance de la base de données utilisées par l'institution.

Les interventions de maintenance sont transcrites dans un registre ad hoc.

Exemples de clauses de sécurité et de confidentialité à prévoir avec le sous-traitant

Chaque opération de maintenance devra faire l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants, transmis à ……, responsable du service informatique, et ……, responsable du traitement des données.

En cas de télémaintenance permettant l'accès à distance aux fichiers de l'institution, le sous-traitant prendra toutes les dispositions nécessaires afin de permettre à l'institution d'identifier la provenance de chaque intervention extérieure. A cette fin, le sous-traitant s'engage à obtenir l'accord préalable de ……, responsable du service informatique, et ……, responsable du traitement des données, avant chaque opération de télémaintenance dont elle prendrait l'initiative.

Des registres seront établis sous les responsabilités respectives de l'institution et du sous-traitant, mentionnant les date et nature détaillée des interventions de télémaintenance ainsi que le nom de leurs auteurs.

Dans le cadre de l'exécution du contrat, le sous-traitant agira uniquement sur les instructions de l'institution. A ce titre, le sous-traitant s'engage à ne pas utiliser les données pour son propre compte ou pour celui d'un tiers.
Conformément au RGPD, le sous-traitant s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment de les protéger contre toute destruction accidentelle ou illicite, perte accidentelle, altération, diffusion ou accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ou communication à des personnes non autorisées.

Le sous-traitant s'engage à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin de protéger la confidentialité des informations auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.
Le sous-traitant s'engage en particulier à :

- *ne pas utiliser les données auxquelles il peut accéder à des fins autres que celles prévues par ses attributions ;*
- *ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions ;*
- *ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de ses fonctions ;*
- *prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;*
- *prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;*

- *s'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;*
- *en cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.*

Cet engagement de confidentialité, en vigueur pendant toute la durée de la présente convention, demeurera effectif, sans limitation de durée après la cessation de la convention, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

Gestion de la sous-traitance

En tant que responsable de traitement, l'institution peut faire appel à un sous-traitant qui, pour remplir les missions qui lui incombent, peut disposer de données personnelles traitées par le responsable de traitement.

Entre autres choses, l'institution, en tant que responsable de traitement a recours à un sous-traitant :

- pour la gestion sociale et fiscale des travailleurs salariés de l'institution ;
- pour le suivi informatique des bases de données de l'institution ;
- …… à compléter si nécessaire

Cette relation avec le sous-traitant fait l'objet d'une convention qui clarifie les responsabilités respectives, la sécurisation des données personnelles tant auprès du responsable de traitement qu'auprès du sous-traitant, le nécessaire respect de la confidentialité,…

Vous trouverez ci-dessous un modèle de convention entre un responsable de traitement et un sous-traitant (source : CNIL)

Entre l'asbl (nom et raison sociale) ……
Située rue ……, n° …….
Code postal …… Commune ……..
Représentée par (nom et fonction) ……
ci-après dénommée « le responsable de traitement »

ET

La société (nom et raison sociale) ……..
Située rue ……, n° …….
Code postal …… Commune ……..
Représentée par (nom et fonction) ……
ci-après dénommée « le sous-traitant »

Il est convenu ce qui suit :

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.
Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (RGPD).

II. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) :

- *Tous les services demandés à un secrétariat social ou à un service social équivalent.*

La ou les finalité(s) du traitement sont :

- *Gestion sociale, fiscale et juridique de la relation contractuelle entre un employeur et ses travailleurs salariés*

La nature des opérations réalisées sur les données est :

- *Vérification du respect des conditions d'engagement ;*
- *Gestion sociale et fiscale des données (gestion des salaires, gestion des documents sociaux et de la déclaration – électronique ou non - des suspensions du contrat de travail, établissement des fiches fiscales, gestion des remboursements de frais, gestion des éléments imposés par la législation relative au bien-être au travail,….) ;*
- *Gestion des données indispensables à un suivi juridique de la relation de travail ;*
- *Gestion de la fin de la relation contractuelle ;*
- *Toute opération imposée par la législation en vigueur et relative à la relation contractuelle entre un employeur et un travailleur salarié ;*
- *Toute opération imposée par la législation en vigueur et relative aux organes de décision de l'institution ;*
- *Toute opération imposée par la législation en vigueur et relative à la relation contractuelle entre un employeur et un travailleur indépendant, un bénévole, un artiste,….*

Les données à caractère personnel traitées sont :

- *Les données liées à l'identité de la personne concernée : nom t prénom, sexe, état civil, données d'identification (adresse, GSM, courriel,…), numéro de registre national, nationalité, carte de séjour et permis de travail,…. ;*
- *Les données relatives au statut de la personne : données requises pour l'octroi d'une aide à l'emploi, parcours scolaire et niveau de diplôme,…. ;*
- *Les données administratives : justificatifs d'absence, compte bancaire, organismes et/ou administrations relais pour l'ouverture ou le maintien de droits sociaux, copie carte d'identité,…. ;*
- *Les données nécessaires pour la mise à disposition des équipements de protection individuelle (EPI) : pointure, allergies de la peau éventuelle,…. ;*
- *Les données salariales : niveau de rémunération, retenues sur salaire, avantages de toute nature ou extralégaux, compte individuel,….. ;*
- *Les données fiscales : fiche fiscale 281.10, remboursement de frais, avantage de toute nature,…..*

Les catégories de personnes concernées sont :

- *Toutes les personnes ayant une relation contractuelle avec le responsable de traitement en tant que travailleur salarié, travailleur indépendant, bénévole, artiste, article 17, tout autre statut mis en place par le législateur et impliquant une intervention d'un secrétariat social.*

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes :

- *Toutes les données reprises ci-avant et nécessaires à l'exécution des obligations du sous-traitant, ainsi que toutes les données non mentionnées mais qui s'imposeront à l'avenir pour la gestion sociale et fiscale de la relation contractuelle entre le responsable de traitement et les catégories de personnes concernées mentionnées ci-avant.*

III. Durée du contrat

La durée du présent contrat est liée à la durée de la convention définissant la relation contractuelle quant au travail à fournir de part et d'autre, et donc du maintien du sous-traitant en tant que secrétariat social du responsable de traitement.

IV. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. *traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance*
2. *traiter les données **conformément aux instructions** du responsable de traitement. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données, il en informe immédiatement le responsable de traitement.*
3. *garantir la **confidentialité** des données à caractère personnel traitées dans le cadre du présent contrat*
4. *veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent contrat :*
   - *s'engagent à respecter la **confidentialité** ou soient soumises à une obligation légale appropriée de confidentialité*
   - *reçoivent la **formation** nécessaire en matière de protection des données à caractère personnel*
5. *prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de **protection des données dès la conception** et de **protection des données par défaut***

Dans la mesure où le sous-traitant accède directement aux données reprises dans la base de données du responsable de traitement, vous pourriez reprendre à cet endroit la clause de sécurité et de confidentialité reprise à la fiche précédente intitulée « encadrement de la maintenance et de la destruction des données ».

*6. **Sous-traitance***

*Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « **le sous-traitant ultérieur** ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai de 15 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.*

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en oeuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

*7. **Droit d'information des personnes concernées***

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

*8. **Exercice des droits des personnes***

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent directement auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à […] (indiquer un contact au sein du responsable de traitement).

9. ***Notification des violations de données à caractère personnel***

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par le moyen suivant [courriel électronique adressé à ……..]. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

10. ***Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations***

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données, si cela s'avère nécessaire.
Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle si celle-ci s'avère nécessaire.

11. ***Mesures de sécurité***

Le sous-traitant s'engage à mettre en oeuvre les mesures de sécurité suivantes :
……
[Vous devez décrire les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres

- *la pseudonymisation et le chiffrement des données à caractère personnel*
- *les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;*
- *les 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;*
- *une procédure visant à tester, à 'analyser et à 'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement]*

Vous pouvez vous référer aux points précédents du présent document et reprendre les items pertinents dans ce cadre.

12. ***Sort des données***

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant conserve les données personnelles tant que les délais de prescription en lien avec les législations imposant la collecte de ces données personnelles ne sont pas atteints ou tant qu'une procédure judiciaire est en cours.

Attention : juridiquement, on doit prévoir, à terme, la destruction des données personnelles. Cette destruction doit pouvoir être justifiée par le sous-traitant.

13. ***Délégué à la protection des données***

Le sous-traitant ne faisant pas de profilage et n'effectuant aucun traitement à grande échelle de données sensibles, il ne dispose pas de délégué à la protection des données.

La personne de contact dans le cadre du RGPD et de la présente convention est :

- *pour le sous-traitant : …….. ;*

- *pour le responsable de traitement : ……..*

14. ***Documentation***

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations (registre de traitements, moyens de sécurité informatique et de l'information mis en œuvre,…) et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

V. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :
1. fournir au sous-traitant les données visées au point II des présentes clauses ;
2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant, mais aussi de sa part en tant que responsable de traitement ;
4. superviser le traitement.

Sécurisation des échanges avec d'autres organismes

Ce point concerne principalement les structures qui doivent, de par leur « corps business », garantir une politique de sécurité plus pointue. On pense, par exemple, aux secrétariats sociaux.

Ce point est à construire avec votre service informatique.

On pourrait retrouver les éléments suivants :

- ne pas utiliser d'adresse mail type « gmail » ou autre messagerie grand public ;
- chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers (DVD, clé USB, disque dur externe,….) ;
- chiffrer les pièces sensibles à transmettre si cette transmission utilise la messagerie électronique ;
- utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers, en utilisant les versions les plus récentes des protocoles (exemple : SFTP, HTTPS) ;
- assurer la confidentialité des secrets (clé de chiffrement, mot de passe,…) en les transmettant via un canal distinct (exemple : envoi du fichier chiffré par courriel et communication du mot de passe par téléphone ou SMS) ;
- signature électronique lors de l'envoi des données qui garantit l'origine du message ;
- ….

Protection des locaux

La sécurisation des locaux, que ce soit les endroits où se trouvent les serveurs, ou les bureaux où se trouvent les données personnelle « version papier »,… est impérative.

Parmi les mesures « de base » possibles, l'on peut citer :

- L'institution a placé des alarmes anti-intrusion vérifiées périodiquement ;
- L'institution dispose de détecteurs de fumée ainsi que des moyens de lutte contre les incendies ;
- La pièce réservée au serveur informatique et aux back up n'est accessible qu'aux personnes habilitées, avec traçabilité de leur passage et interventions ;
- Le matériel informatique dispose de moyens de protection spécifiques (exemples : système anti-incendie spécifique, surélévation de ce matériel contre d'éventuelles inondations, redondance d'alimentation électrique et/ou de climatisation,…).

Encadrement des développements informatiques

Ce point ne concerne que les institutions qui développent des programmes ou des bases de données informatiques. A voir avec votre service informatique.

Si vous êtes concerné, vous devez prévoir l'intégration de la protection des données privées, y compris ses exigences de sécurité des données, dès la conception de l'application ou du service informatique. Ces exigences peuvent se traduire par des choix d'architecture (décentralisée vs centralisée), de fonctionnalités (anonymisation à bref délai, minimisation des données), de technologies (chiffrement des communications),….

Chiffrement, garantie de l'intégrité, signature

Ce point concerne principalement les structures qui doivent, de par leur « corps business », garantir une politique de sécurité plus pointue. On pense, par exemple, aux secrétariats sociaux.

Ce point est à construire avec votre service informatique.

Les fonctions de hachage permettent d'assurer l'intégrité des données.

Les signatures numériques, en plus d'assurer l'intégrité, permettent de vérifier l'origine de l'information et son authenticité.

Le chiffrement permet de garantir la confidentialité d'un message.

Droit des personnes dont des données personnelles ont été collectées et traitées

---

Toute personne ayant communiqué des données personnelles, y compris les travailleurs de l'institution pour leurs propres données, disposent des protections suivantes :

Droit d'accès et de rectification des données

A tout moment, vous pouvez prendre contact avec …….. (nom, titre et ou fonction et moyens de contact) afin de connaître les données personnelles dont dispose l'institution, la façon dont ces données sont conservées. A ce droit d'accès est lié un droit de rectification s'il s'avère que ces données sont obsolètes.

Droit de portabilité

Chaque personne concernée a le droit, pour ce qui le concerne :

- de recevoir ses propres données dans un format structuré, couramment utilisé et lisible par une machine (PC) ;
- et si c'est techniquement possible, d'obtenir que les données soient directement transmises à un autre responsable de traitement (ceci ne vise que les données dont le responsable de traitement dispose en raison du consentement écrit de la personne concernée et pour lesquelles le traitement est effectué à l'aide de procédés automatisés).

Droit à l'effacement (ou droit à l'oubli numérique)

Toute personne concernée a le droit d'obtenir l'effacement de ses données dans les meilleurs délais dans les cas suivants :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités poursuivies ;
- elle retire le consentement sur lequel est fondé le traitement ;
- elle s'oppose au traitement de ses données à des fins de prospection ;
- les données ont fait l'objet d'un traitement illicite ;
- les données ont été collectées dans le cadre de l'offre directe de service à un enfant de moins de 16 ans.

Le droit à l'effacement ne concerne donc pas les données personnelles récoltées dans le cadre de la gestion sociale et fiscale des travailleurs salariés.

Désignation d'un délégué de protection des données (DPD ou DPO)

La désignation d'un délégué à la protection des données (DPD) est obligatoire dans les cas suivants :

- le traitement des données à caractère personnel est effectué par une autorité publique ou un organisme public ;
- les activités de base du responsable de traitement 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 (profilage) ;
- les activités de base du responsable de traitement consistent en un traitement à grande échelle de catégories particulières de données (données sensibles).

L'institution n'est pas un organisme public. Elle ne collecte aucune donnée sensible et ne conserve les données personnelles que pour répondre adéquatement à ses missions et à son but social, sans aucune visée de profilage.

L'institution n'est donc pas tenue de disposer d'un délégué à la protection des données.

En raison de la petitesse de la structure, du peu de données personnelles récoltées et des moyens financiers disponibles, l'institution décide de ne pas engager de DPD.

L'institution veille toutefois à conscientiser, informer, former et suivre les travailleurs de l'institution collectant et traitant ces données personnelles.