PROCÉDURE D'ACCUEIL DES STAGIAIRES ET PROTECTION DES DONNÉES

CONFIDENTIALITÉ ET SÉCURITÉ DU PARCOURS

Accueillir avec attention, protéger les informations



Accueil et confidentialité

Accueil et intégration

1. Objet et champ d'application

Cette procédure définit les règles à suivre lors de l'accueil des apprenants et stagiaires au sein de l'organisme, afin de garantir un accompagnement de qualité tout en assurant la confidentialité et la sécurité des données personnelles collectées, conformément au RGPD.

Elle s'applique à tout le personnel de l'organisme de formation (formateurs, administratifs, direction) ainsi qu'aux sous-traitants.

2. Phase d'accueil et d'intégration

2.1. Avant la formation

Information préalable : envoyer aux stagiaires la convocation, le règlement intérieur et les conditions générales de vente (CGV).

Mention RGPD : s'assurer que le formulaire d'inscription contient la mention d'information sur le traitement des données : finalités, durée de conservation et droits d'accès.

2.2. Le premier jour de formation

Vérification d'identité et émargement : recueillir la signature sur la feuille d'émargement. Ce document doit rester sous la surveillance du formateur.

Briefing de rentrée : rappeler le programme, les règles de sécurité et les consignes de confidentialité au sein des locaux ou de la plateforme de formation en ligne.

Gestion et protection des données

3. Gestion et protection des données personnelles (RGPD)

3.1. Données collectées

Le centre collecte uniquement les données strictement nécessaires (principe de minimisation).

Identité : nom, prénom, date de naissance, coordonnées (courriel, téléphone).
Suivi pédagogique : profil professionnel, niveau d'études, évaluations, assiduité (feuilles d'émargement).

3.2. Finalités du traitement

Gestion administrative et pédagogique des formations.
Déclaration d'assiduité auprès des organismes financeurs (OPCO, France Travail, Région, etc.).
Amélioration des prestations par les enquêtes de satisfaction.

3.3. Mesures de sécurité des données

Supports papier (feuilles d'émargement, dossiers) : stockage dans des armoires fermées à clé et destruction par broyage.

Partage de données : interdiction d'envoyer des fichiers contenant des données sensibles par un canal non sécurisé.

Accès aux locaux : accueil filtré. Les visiteurs externes ne doivent pas voir les écrans du personnel.

3.4. Durée de conservation des données

Dossiers pédagogiques et administratifs : conservation pendant 5 ans après la fin de la formation (durée de contrôle indiquée dans la procédure source).

Droits et gestion des incidents

4. Droits des stagiaires

Chaque stagiaire dispose d'un droit d'accès, de rectification, d'effacement et de portabilité de ses données.

5. Cas particulier : droit à l'image et enregistrements

Formations en présentiel : aucune photo ou vidéo ne peut être prise et diffusée (réseaux sociaux, site web) sans l'accord écrit préalable du stagiaire via un formulaire d'autorisation de droit à l'image.

Classes virtuelles : si la session est enregistrée pour un replay, les stagiaires doivent en être informés au début. Ils ont le droit de couper leur caméra et leur micro si l'enregistrement n'est pas une condition obligatoire du parcours.

6. Gestion des violations de données

En cas de perte, de vol ou de fuite de données (par exemple : piratage informatique, vol d'un ordinateur) :

1. Informer immédiatement le responsable du centre de formation.

2. Documenter l'incident dans le registre interne des violations.

3. Si la violation présente un risque pour les droits des personnes, notifier la CNIL sous 72 heures et avertir les stagiaires concernés.