GESTION ET PROTECTION DES RENSEIGNEMENTS PERSONNELS D'EMPLOYÉS EN ENTREPRISE

LOI 25

RENSEIGNEMENT PERSONNEL

Chez Ciao, nous accordons une grande importance à la confidentialité des données des futurs employés, employés et anciens employés. C'est pourquoi nous mettons en place des mesures visant à garantir la protection des informations personnelles que vous nous confiez.

Dans le cadre de votre emploi, Ciao collectera des renseignements personnels pour mener à bien ses offres de services et respecter ses obligations légales.

RENSEIGNEMENT PERSONNEL
INDIVIDUEL

- Nom
- Âge
- Éducation
- NAS
- Pièce d'identité
- No compte
- No de permis
- Date de naissance
- Antécédents criminels
- Spécimen de chèque
- Revenus
- Bonus
- Performance
- Opinion
- Placement
- Titre
- Adresse
- Numéro de téléphone
- Adresse courriel
- Renseignements sur les plaintes
- Adresse protocole Internet (IP)
- Informations sur la santé physique ou mentale de l'employé
- Niveau d'emploi
- Etc.

LES PRINCIPES DE BASE EN MATIÈRE DE PRP

Nous mettons le consentement au cœur de nos pratiques en matière de renseignements personnels, en veillant à ce que la collecte, l'utilisation et la communication de ces données se fassent uniquement avec le consentement de l'individu, sauf dans les cas prévus par la loi. Notre engagement s'étend également à la préservation de l'exactitude, de la conservation et de la sécurité des informations, garantissant ainsi le respect absolu de la vie privée de nos employés.

RENSEIGNEMENT PERSONNEL RECRUTEMENT

Dans le cadre de notre processus de recrutement, nous accordons une grande importance aux renseignements personnels. Nous tenons compte des éléments suivants :

- **Les renseignements d'un curriculum vitae**
  Nous examinons attentivement les informations fournies dans les CV des candidats pour évaluer leur adéquation au poste.

- **Le caractère public d'un renseignement personnel**
  Nous nous assurons de respecter les limites de ce qui est considéré comme des informations personnelles publiques, en accordant une attention particulière à la confidentialité des données sensibles.

- **Les questions en entrevue et la collecte accessoire d'information**
  Nous posons des questions pertinentes et nécessaires lors des entretiens pour mieux comprendre les compétences et l'expérience des candidats, tout en respectant la vie privée.

- **Risque de discrimination (Chartes)**
  Nous nous conformons aux lois et aux chartes anti-discrimination pour garantir un processus de recrutement équitable et respectueux de la diversité.

- **Recrutement par des tiers (firme de recrutement)**
  Lorsque nous faisons appel à des tiers, tels que des firmes de recrutement, nous nous assurons qu'ils respectent les mêmes normes de protection des données personnelles que nous.

RENSEIGNEMENT PERSONNEL RÉFÉRENCEMENT

Dans le cadre d'un référencement, qu'il soit effectué par un employé de l'entreprise ou par un tiers, nous accordons une priorité absolue à la confidentialité des renseignements personnels. Il est important de noter que le référencement post-emploi peut également être inclus dans cette procédure. Dans ce contexte, nous prenons en considération les éléments suivants :

- Le référencement de candidat par un employé

  Lorsqu'un employé de notre entreprise ou un tiers nous référence un candidat, il doit envoyer sa candidature au département des ressources humaines pour garantir que l'information partagée est pertinente, précise et basée sur des observations professionnelles.

- Nature des renseignement nécessaires

  Lorsqu'un employé de notre entreprise ou un tiers nous référence un candidat, nous leur demandons de fournir des informations pertinentes et professionnelles concernant le candidat. Nous insistons sur l'importance de ne pas inclure d'informations personnelles ou confidentielles qui ne sont pas directement liées à l'évaluation professionnelle du candidat.

- Consentement

  Lors du référencement, que ce soit avant l'embauche (pré-emploi) ou après l'embauche (post-emploi), le département des ressources humaines veille à obtenir préalablement le consentement du candidat. Cette étape essentielle garantit que le candidat est pleinement informé de la procédure de référencement et qu'il donne son accord explicite pour la collecte et le partage de ses informations professionnelles.

RENSEIGNEMENT PERSONNEL RÉFÉRENCEMENT

- Ordre des événements :

  Le référencement doit être effectué de manière ordonnée et éthique. Cela signifie que le processus de recrutement, y compris les entretiens et les évaluations internes, doit être mené avant le référencement. Cette séquence garantit que les candidats sont évalués sur la base de leurs compétences et de leurs qualifications avant que des informations tierces ne soient prises en compte.

- Recrutement par des tiers (firme de recrutement)

  Lorsque des renseignements sur un candidat sont obtenus auprès de tiers, tels que d'anciens employeurs, nous nous assurons de respecter les lois et réglementations en matière de confidentialité des données. Les informations collectées de cette manière sont utilisées uniquement dans le cadre du processus de recrutement et sont conservées de manière sécurisée. Nous veillons également à ne pas utiliser ces informations pour des motifs autres que l'évaluation professionnelle du candidat.

À L'EMPLOI CHEZ CIAO

Les renseignements personnels en milieu d'emploi

RENSEIGNEMENT PERSONNEL EN MILIEU D'EMPLOI

À l'emploi chez Ciao, nous recueillons les données personnelles individuelles de nos employés afin de garantir le bon fonctionnement de l'entreprise et de répondre à nos obligations légales. Les informations que nous collectons sont les suivantes :

- **Données socio-démographiques:**

  Cela inclut des informations telles que le nom, le prénom, la date de naissance, l'adresse, etc.

- **Identifiant unique**

  Nous collectons des identifiants uniques tels que le numéro d'assurance sociale (NAS), les numéros de permis, le spécimen de chèque, etc.

- **Informations liées à la santé:**

  Nous recueillons des informations concernant la santé des employés, notamment en ce qui concerne les absences prolongées et les informations liées à l'assurance collective.

- **Information du dossier d'antécédents, le cas échéant:**

  Si cela est pertinent pour la nature du poste ou les exigences légales, nous pouvons collecter des informations liées aux antécédents des employés.

RENSEIGNEMENT PERSONNEL EN MILIEU D'EMPLOI

- Information financière

  Cela inclut des détails sur le salaire, les bonus, les indicateurs de performance et d'autres informations financières pertinentes.

- Déplacements

  Nous recueillons des informations sur les déplacements professionnels des employés, notamment les frais de déplacement, les itinéraires et les notes de frais, le cas échéant.

- Toute autre information pertinente pour l'employeur dans le cadre légal:

  Nous pouvons collecter d'autres informations qui sont nécessaires pour la gestion de l'administration et des ressources humaines et qui sont conformes aux lois et réglementations en vigueur.

LA GESTON DES ACCÈS

LES ÉLÉMENTS À SAVOIR

LA GESTION DES ACCÈS

La gestion des accès est cruciale pour assurer la sécurité de l'entreprise. Elle repose sur un contrôle rigoureux à deux niveaux : lors de l'embauche des employés et par le biais de vérifications en cours d'année. Voici les éléments clés de cette gestion :

- **L'accès aux ressources protégées des employés :**

  Les employés ont des accès appropriés aux ressources et aux données de l'entreprise en fonction de leurs fonctions. Cela signifie que l'accès aux informations sensibles sont limité aux personnes qui en ont besoin pour accomplir leurs tâches.

- **Gestion des accès :**

  Un processus est mis en place pour attribuer et révoquer les droits d'accès de manière appropriée. Cela implique la création de comptes, l'attribution de privilèges et l'activation de mesures de sécurité comme l'authentification à deux facteurs.

- **Suivi et mise à jour des accès :**

  Les droits d'accès sont régulièrement surveillés pour s'assurer qu'ils sont toujours appropriés. Lorsque les responsabilités d'un employé changent ou lorsque des employés quittent l'entreprise, les droits d'accès sont ajustés en conséquence..

- **Mesures de contrôle et de mitigation :**

  Des mesures de contrôle sont mises en place pour prévenir les accès non autorisés. Cela peut inclure la détection d'intrusions et l'application de politiques de sécurité strictes.

LES BRIS DE CONFIDENTIALITÉS

Un bris de confidentialité survient lorsque des informations confidentielles, privées ou sensibles sont divulguées, partagées, consultées ou utilisées de manière non autorisée ou inappropriée. Ces données peuvent englober des informations personnelles, médicales, financières, professionnelles ou d'autres types de renseignements confidentiels.

LA CONFIDENTIALITÉ

Quelques exemples de bris de confidentialité

- Mauvais destinataires lors de transmission de courriels ou de courriers (ex. : fonctions Cc / Cci, sélection automatique, erreurs d'écriture, etc.);
- Divulgation de renseignements personnels à une personne non autorisée;
- Consultation non autorisée par un employé;
- Perte ou vol d'un envoi postal, bac de recyclage non cadenassé;
- Vol ou perte de matériel informatique (clés USB, autres médias amovibles);
- Etc.

QUOI FAIRE EN CAS D'INCIDENT PRP?

En cas de bris de confidentialité, il est essentiel d'adopter une approche immédiate pour atténuer les impacts potentiels et protéger les informations confidentielles.

INCIDENT PRP?

Voici quelques étapes à suivre en cas de bris de confidentialité:

- **Notification aux personnes visées :**

  Il est essentiel de notifier rapidement les personnes dont les données ont été compromises. La notification doit comporter des informations détaillées sur la nature de la violation ainsi que les données potentiellement affectées. De plus, il est également de la responsabilité de toute tierce partie détenant ces données de prendre des mesures immédiates pour supprimer les courriels ou les données en sa possession.

- **Mise en place d'un registre :**

  Ciao maintient un registre détaillé des incidents liés aux bris de confidentialité des données. Ce registre joue un rôle essentiel dans l'évaluation post-incident et nous aide à respecter nos obligations légales en matière de déclaration. Il nous permet également d'intervenir rapidement pour minimiser les répercussions des incidents.

- **Informer le responsable PRP:**

  En fonction de la gravité de l'incident, il peut être nécessaire d'informer le responsable de la protection des renseignements personnels au sein de l'entreprise. Chez Ciao, un responsable spécialement désigné est en charge de coordonner la réponse à l'incident. Il assure également que nous sommes en conformité avec toutes les obligations légales et réglementaires en matière de protection des données. Ce responsable supervise toutes les actions de l'entreprise pour garantir la sécurité des données dans le cadre de la gestion d'incident.

FIN D'EMPLOI

Lorsqu'un employé quitte l'entreprise, les données relatives à cet employé sont conservées dans la base de données de l'entreprise pendant une période de dix (10) ans. Cette conservation vise à des fins de référencement, de statistiques, d'obligation gouvernementale et à des fins administratives. À l'expiration de cette période, Ciao s'engage à supprimer ou à anonymiser ces renseignements de manière sécurisée, sauf si leur conservation est requise par la loi.

CONSERVATION & ACCÈS

Ciao conserve plusieurs éléments liés aux employés et à leur emploi. Voici quelques exemples de données typiquement conservées :

- La conservation des renseignements:

  En général, les éléments évoqués dans ce document, notamment le contrat de travail, les évaluations de performance, les données fiscales et de rémunération, ainsi que les dossiers médicaux, font l'objet d'une conservation rigoureuse en accord avec les réglementations légales et les politiques internes de l'entreprise. La conservation des données relatives aux candidats non retenu sont également assujetti à cette politique.

- Méthode de destruction:

  Lorsque le délai de conservation est atteint, Ciao a mis en place une procédure de destruction des données confidentielles et des documents, veillant à ce qu'ils ne puissent pas être récupérés ni utilisés de manière inappropriée. La destruction peut être réalisée par le biais de déchiquetage, de la suppression des dossiers informatiques ou de l'anonymisation des documents, selon les exigences spécifiques pour chaque type de données et conformément aux meilleures pratiques en matière de sécurité des données.

LA PRÉSENTATION A ÉTÉ SOIGNEUSEMENT PRÉPARÉE PAR L'ÉQUIPE CIAO. NOUS VOUS REMERCIONS DE L'AVOIR CONSULTÉE.