

Politique de confidentialité



MACPEK
PIÈCES VÉHICULES LOURDS

Table des matières

1. Contexte	2
2. Objectif de la politique et définition	2
3. Renseignements personnels recueillis et ce pourquoi nous les recueillons	2
4. La façon dont nous recueillons des renseignements personnels.....	6
5. Personnes ayant l'accès aux renseignements personnels.....	8
6. Mesures de sécurité	9
7. Conservation.....	12
8. Les droits des personnes concernées par les renseignements personnels.....	12

1. Contexte

Chez Macpek Inc., distributeur de pièces pour véhicules lourds (ci-après « Macpek »), le respect de la vie privée et la protection des renseignements personnels de nos clients, employés, fournisseurs et partenaires d'affaires sont des priorités fondamentales. Nous reconnaissons l'importance de traiter ces renseignements de manière responsable, sécuritaire et transparente, conformément aux exigences de la Loi 25.

2. Objectif de la politique et définition

La présente politique a pour objectif de garantir la protection des renseignements personnels et de définir clairement les pratiques de Macpek en matière de collecte, d'utilisation, de communication, de conservation, de destruction ou de gestion plus générale de ces renseignements. Elle vise aussi à informer toute personne concernée sur la manière dont Macpek traite ses données personnelles, les droits dont elle dispose à cet égard et les mesures mises en place pour assurer leur confidentialité.

Les renseignements personnels visés sont ceux qui permettent d'identifier directement ou indirectement une personne physique. Ces renseignements sont traités avec rigueur et demeurent confidentiels.

3. Renseignements personnels recueillis et ce pourquoi nous les recueillons

3.1. Types de renseignements recueillis et pourquoi ces renseignements sont recueillis

Renseignements collectés auprès des employés

Dans le cadre de la gestion de la relation d'emploi, nous recueillons différents types de renseignements personnels, nécessaires pour assurer une gestion efficace et conforme des ressources humaines, de la paie, des régimes collectifs et de la conformité réglementaire.

Renseignements d'identification

Ces renseignements sont utilisés pour la gestion du dossier employé, la paie, l'administration des assurances collectives et du régime de retraite. Ils incluent le nom et prénom, l'adresse du domicile, la date de naissance, le numéro de téléphone ainsi que l'adresse courriel personnelle.

Renseignements relatifs à l'emploi et au parcours académique

Ces données sont requises pour des fins de gestion des ressources humaines, de rémunération, d'administration des avantages sociaux, de confirmation d'emploi, de vérifications des références, ainsi que pour répondre aux obligations légales et réglementaires. Elles incluent le poste occupé, la fonction ou le titre, le salaire, l'historique d'emploi ainsi que le parcours académique et les formations.

Renseignements administratifs et financiers

Ces données permettent le traitement de la paie, l'émission des relevés fiscaux et le traitement de certains dossiers d'invalidité. Elles incluent le numéro d'assurance sociale et les coordonnées bancaires.

Renseignements médicaux et de santé

Dans certaines situations, des renseignements médicaux peuvent être utilisés à des fins de gestion des absences pour raisons médicales, de traitement des dossiers d'accident de travail et d'invalidité. Ils incluent notamment les billets médicaux et les formulaires d'invalidité.

Renseignements spécifiques à certains postes

Le numéro de permis de conduire est recueilli pour les postes où la conduite d'un véhicule est exigée. Cette information est utilisée pour vérifier périodiquement la validité du permis et assurer notre conformité aux exigences d'assurance.

Renseignements personnels concernant des tiers

Ces données sont recueillies afin d'assurer une communication rapide en cas d'urgence et pour l'administration des régimes collectifs. Elles incluent le nom et les coordonnées des personnes à contacter en cas d'urgence ainsi que certains renseignements sur les personnes à charge ou les bénéficiaires.

Renseignements personnels recueillis auprès des clients et des fournisseurs

Dans le cadre de nos activités commerciales, nous collectons certains renseignements personnels relatifs aux clients et fournisseurs. Ces informations sont nécessaires pour assurer la bonne gestion des comptes, le traitement des paiements, la gestion du crédit et le respect de nos obligations contractuelles et légales.

Renseignements financiers liés aux paiements

Ces informations sont utilisées uniquement pour effectuer ou recevoir des paiements de la part de nos clients, dans un cadre sécurisé. Elles incluent le numéro de carte de crédit, le nom du détenteur de la carte, la date d'expiration ainsi que le code de sécurité (CVV).

Renseignements bancaires et de facturation – clients et fournisseurs

Ces renseignements sont conservés afin de gérer leurs comptes, assurer le suivi des paiements et procéder à la facturation. Ils incluent les coordonnées bancaires des clients, les renseignements personnels des clients (tels que le nom, l'adresse et les coordonnées), ainsi que le nom, l'adresse et les coordonnées bancaires des fournisseurs. Les coordonnées bancaires de nos fournisseurs sont conservées dans le but de traiter les paiements qui leur sont dus de manière efficace et conforme.

Gestion du crédit et du risque client

Ces informations sont utilisées dans le cadre de la gestion du crédit, la prévention du risque, le suivi des comptes clients et l'évaluation de la solvabilité. Elles incluent les données liées aux contrats clients, telles que l'ouverture de compte, les comptes en consignation et l'adhésion au programme Mekpro. Elles comprennent également le nom, l'adresse, le solde du compte, l'historique de crédit et les coordonnées des clients. Enfin, elles peuvent inclure des données recensant l'historique de clients, ce qui peut parfois contenir des renseignements personnels, de crédit ou bancaires.

Renseignements personnels recueillis en ligne

Dans le cadre de ses responsabilités, le département des technologies de l'information recueille certains renseignements personnels afin d'assurer la gestion des accès numériques, la communication avec les utilisateurs et la participation à différents services numériques.

Utilisation du site d'e-commerce

Lors de l'utilisation de la plateforme d'e-commerce, l'adresse courriel des utilisateurs est enregistrée puisqu'elle sert de nom d'utilisateur pour l'accès au site. De plus, la date et l'heure de connexion sont automatiquement enregistrées afin d'assurer la sécurité et la traçabilité des activités sur la plateforme.

Communications électroniques

L'adresse courriel est également recueillie lorsqu'une personne s'inscrit à notre infolettre ou à l'une de nos formations. Ces renseignements sont nécessaires pour permettre l'envoi des communications pertinentes aux utilisateurs concernés.

Témoins de connexion (cookies)

Ces renseignements sont recueillis afin de comprendre comment les visiteurs interagissent avec le site web et d'améliorer l'expérience utilisateur. Ils sont collectés par l'intermédiaire d'un outil qui enregistre des données non personnelles liées à la navigation. Ces données incluent les pages consultées, la durée des visites, le type d'appareil utilisé, le navigateur, ainsi que le site référent.

3.2. Mesures offertes pour refuser la collecte de certains renseignements personnels

Dans certains cas, les personnes concernées peuvent refuser de fournir des renseignements personnels. Lorsque cela est possible, nous offrons des mesures concrètes pour permettre ce choix, dans le respect de la loi et des exigences de nos services.

Option de retrait du consentement

Lorsqu'un renseignement est recueilli à des fins de marketing, les personnes peuvent retirer leur consentement à tout moment via un lien de désabonnement.

Choix au moment de l'inscription

Dans certains cas, les participants peuvent choisir de ne pas fournir tous les renseignements.

Refus des témoins non essentiels

Lors de la première visite sur notre site, les utilisateurs peuvent refuser l'utilisation des témoins (cookies) non essentiels en utilisant la bannière de consentement affichée. Il est également possible de modifier ces préférences ultérieurement via les paramètres du navigateur.

Choix de ne pas transmettre certains documents médicaux

Selon la situation, il est possible de choisir de ne pas fournir certains renseignements médicaux ou documents, notamment lorsque leur transmission n'est pas obligatoire.

3.3. Conséquences possibles du refus de fournir certains renseignements

Refuser de fournir certains renseignements personnels peut entraîner des conséquences, selon le type de renseignement et le contexte.

Impossibilité d'accéder à certains services

Certains renseignements sont essentiels pour l'exécution d'un contrat ou la prestation d'un service.

Limitations fonctionnelles

Le refus de partager certaines informations pourrait restreindre l'accès aux différents outils, formations ou communications.

Retrait de certains avantages

Dans le cadre des programmes d'assurance collective ou de régime de retraite, refuser de fournir des renseignements obligatoires pourrait limiter l'admissibilité ou le traitement de certaines réclamations.

Retards dans le traitement

Si des renseignements sont requis pour une vérification, leur absence pourrait retarder l'entrée en fonction ou certaines démarches administratives.

Prise en charge individuelle de certaines démarches

En cas de refus de transmettre certains renseignements, la personne concernée pourrait devoir assumer elle-même l'ensemble des démarches administratives auprès des tiers concernés, y compris la transmission des formulaires, les suivis de dossier et la communication des informations requises.

Dans tous les cas, nous respectons le droit de refuser de fournir certains renseignements. Cependant, certains renseignements sont essentiels à l'exécution de nos obligations contractuelles, légales ou de service.

4. La façon dont nous recueillons des renseignements personnels

La collecte de renseignements personnels s'effectue directement auprès des personnes concernées, selon les modalités suivantes :

Processus de recrutement

- Lors du dépôt d'une candidature sur le site Internet ou par tout autre moyen d'envoi du curriculum vitae.
- Lors du traitement d'une candidature, par le biais de formulaires internes.
- Lors de l'embauche, au moyen de formulaires internes et de la transmission des coordonnées bancaires.

Période d'emploi chez Macpek

- Lors de l'inscription aux régimes collectifs ou lors de la mise à jour de ces régimes, par le biais de formulaires fournis par les tiers concernés.
- Lors du processus de gestion des absences.
- Lors de l'inscription à certaines activités sociales interne.

Partenariat d'affaires

- Lors de la demande d'ouverture de compte client, par le biais de formulaires divers et de la transmission des coordonnées bancaires ou d'informations de carte de crédit.
- Lors de l'inscription à titre de fournisseur, au moyen de formulaires divers et de la transmission des coordonnées bancaires.
- Lors de l'inscription à des formations sur notre site Internet;
- Lors de l'inscription à l'infolettre;
- Lors de transactions effectuées sur notre site d'e-commerce.

4.1. Tiers qui recueillent des renseignements confidentiels pour nous

La collecte de renseignements personnels s'effectue principalement directement auprès des personnes concernées, sauf en cas de consentement donné à un tiers ou lorsque la loi l'autorise.

Agence de placement

Dans le cadre du processus de recrutement, des renseignements personnels peuvent également être transmis par des agences de placement, lorsque ces dernières ont reçu l'autorisation de partager des informations avec Macpek aux fins du traitement de la candidature.

Google Analytics

Nous utilisons Google Analytics pour recueillir des données non personnelles liées à la navigation sur notre site web. Ces données servent uniquement à des fins statistiques et d'amélioration continue de notre site. Aucune information permettant d'identifier directement une personne n'est collectée par cet outil.

5. Personnes ayant l'accès aux renseignements personnels

5.1. Accès aux renseignements personnels au sein de l'entreprise

L'accès aux renseignements personnels est strictement réservé aux personnes autorisées lorsque cet accès est requis dans l'exercice des fonctions pour les fins prévues à la présente politique.

Renseignements collectés auprès des employés

L'ensemble des renseignements est partagé avec l'équipe de gestion des talents. Dans certaines circonstances, une partie de ces renseignements peut également être accessible aux gestionnaires et à l'équipe comptable de l'entreprise.

Renseignements personnels recueillis auprès des clients

L'ensemble de ces renseignements est partagé avec l'équipe comptable ainsi qu'à l'équipe des comptes à recevoir. Certains renseignements relatifs aux informations de paiement sont également accessibles aux équipes en succursale pour le traitement des factures.

Renseignements personnels recueillis auprès des fournisseurs

L'ensemble de ces renseignements est partagé avec l'équipe comptable ainsi qu'à l'équipe des comptes à payer.

Renseignements personnels recueillis en ligne

L'ensemble de ces renseignements est partagé avec l'équipe du support informatique. Les renseignements spécifiques à l'inscription aux formations sont également partagés avec l'équipe de formateurs.

5.2. Tiers avec qui des données confidentielles sont partagées

Aucun renseignement personnel n'est partagé avec des entreprises, des organisations ou des personnes extérieures à Macpek, à l'exception des fournisseurs et partenaires autorisés dont l'accès est nécessaire aux fins énumérées dans la présente politique et dans les limites de celle-ci. Ces tiers peuvent inclure :

- Fournisseurs de service de gestion des candidatures, des dossiers employés et de la paie;
- Fournisseurs de service en matière d'assurances, de régime de retraite et de programme d'aide aux employés;
- Mutuelle de prévention en santé et sécurité au travail;
- Comités paritaires des services automobiles;
- Employeurs;
- Institutions financières;
- Ministères, organismes gouvernementaux ou autorités réglementaires;
- Entreprise en gestion du crédit et du risque client;
- Fournisseurs de service pour la gestion des paiements, clients et fournisseurs;
- Entreprises en matière d'audits financiers et de conformité.

6. Mesures de sécurité

Nous protégeons les renseignements personnels détenus par Macpek contre tout accès non autorisé, toute divulgation, perte ou toute autre forme d'atteinte. Cela inclut :

6.1. Mesures physiques

Protection physique

Les employés ayant accès à des informations confidentielles travaillent dans des bureaux fermés ou disposent de classeurs verrouillés, afin de prévenir tout accès non autorisé et de protéger les documents sensibles.

6.2. Mesures technologiques

Protection de notre réseau contre les attaques extérieures

Nous mettons en place des mesures technologiques pour protéger notre infrastructure informatique contre les attaques extérieures. Nous surveillons continuellement l'activité réseau afin de repérer toute tentative d'intrusion, bloquer les connexions non autorisées ou tout comportement anormal pouvant indiquer une menace potentielle.

Authentification multifactorielle

Nous utilisons l'authentification multifactorielle à tout accès aux données sensibles. L'authentification multifactorielle demande deux preuves d'identité : un mot de passe et un code temporaire reçu sur une application. Cette méthode ajoute un niveau de sécurité supplémentaire qui réduit considérablement les risques d'accès non autorisé, même en cas de vol ou de fuite de mots de passe.

Gestion des accès

Nous accordons aux employés uniquement les accès nécessaires à l'exercice de leurs fonctions. Ce principe limite l'exposition des données en réduisant les accès inutiles, diminuant ainsi les risques d'erreurs, de fuites ou d'abus.

Mises à jour régulières

Nous veillons à mettre à jour nos logiciels et nos systèmes d'exploitation pour corriger les vulnérabilités de sécurité.

Gestion et partage sécurisé des données

Nous protégeons les données personnelles de nos utilisateurs en les hébergeant dans un environnement sûr et confidentiel. Le partage des documents se fait également de manière sécurisée, protégeant la confidentialité et l'intégrité de nos informations tout en favorisant une collaboration efficace.

Mot de passe sur les fichiers partagés par courriel

Nous sensibilisons nos employés à l'importance de protéger les données personnelles en ajoutant un mot de passe aux fichiers envoyés par courriel. Cela permet de réduire les risques de divulgation accidentelle ou d'accès non autorisé à des informations sensibles.

Paieements sécurisés

Nous utilisons une plateforme de paiement sécurisée qui chiffre les informations sensibles dès leur saisie par le client et pendant toute la transmission vers le réseau bancaire.

6.3. Mesures administratives

Système d'information des ressources humaines (SIRH)

Dans le cadre de notre gestion des ressources humaines, nous utilisons un système d'information des ressources humaines (SIRH) pour collecter, traiter et conserver des renseignements personnels sur nos employés. Nous mettons en place des mesures strictes pour assurer la sécurité, la confidentialité et l'intégrité de ces données. Seules les personnes autorisées ont accès au SIRH, et ce, selon des droits d'accès strictement définis en fonction des rôles.

Système de gestion des candidatures (ATS)

Nous utilisons un système de gestion des candidatures (ATS) qui facilite la gestion, la centralisation et le suivi du processus de recrutement, tout en assurant la protection des données personnelles des candidats et la sécurité globale du recrutement.

Système de paie

Nous effectuons le traitement de la paie en utilisant un système qui assure la gestion sécurisée des renseignements personnels de nos employés. L'accès aux données est strictement réservé aux personnes autorisées, en fonction de leur rôle, ce qui réduit les risques de consultation non autorisée.

Système comptable et de gestion des comptes clients

Nous utilisons un système comptable ainsi qu'un logiciel de gestion des comptes clients afin d'assurer la confidentialité et la sécurité des données financières et personnelles de nos clients et fournisseurs. Ces outils protègent l'information tout au long du processus de facturation et d'encaissement, tout en réduisant les risques de fraude. Les droits d'accès sont attribués selon les fonctions des utilisateurs, ce qui permet de limiter les accès non autorisés aux données sensibles.

6.4. Mesures humaines

Sensibilisation des employés

Nous sensibilisons notre personnel aux bonnes pratiques en matière de cybersécurité et de confidentialité afin de réduire les risques liés à l'utilisation inappropriée des outils informatiques. Cette sensibilisation inclut, entre autres, la reconnaissance des courriels frauduleux et des tentatives d'hameçonnage, ainsi que la gestion sécurisée des mots de passe, en soulignant l'importance de leur confidentialité et de leur complexité.

7. Conservation

Nous conservons les renseignements personnels uniquement pour la durée nécessaire à la réalisation des fins pour lesquelles ils ont été collectés, ou tel que requis par les lois et règlements applicables.

Une fois que les renseignements personnels ne sont plus requis, nous nous engageons à les détruire de manière sécuritaire conforme aux pratiques reconnues en matière de protection des données.

8. Les droits des personnes concernées par les renseignements personnels

Conformément à la Loi sur la protection des renseignements personnels dans le secteur privé (Loi 25 – Québec) et aux principes généralement reconnus en matière de protection des données, toute personne dont nous recueillons des renseignements personnels dispose des droits suivants :

Droit à l'information

Il est possible d'être informé de la collecte, de l'utilisation, de la communication et de la conservation des renseignements personnels. Ces informations sont fournies de manière claire et transparente.

Droit d'accès

Il est permis de demander quels renseignements personnels sont détenus à son sujet. Une copie de ces renseignements sera transmise sur demande écrite, sous réserve des exceptions prévues par la loi.

Droit de rectification

Toute personne peut demander la correction de renseignements personnels jugés inexacts, incomplets ou équivoques. Les modifications nécessaires seront apportées dans les meilleurs délais.

Droit de retrait du consentement

Lorsque le traitement des renseignements personnels repose sur le consentement, celui-ci peut être retiré en tout temps. Ce retrait pourrait toutefois restreindre l'accès à certains services.

Droit à la suppression

Dans certaines circonstances, une demande de suppression des renseignements personnels peut être formulée, notamment lorsqu'ils ne sont plus nécessaires aux fins pour lesquelles ils ont été recueillis ou lorsque leur traitement n'est plus justifié.

Droit de déposer une plainte

En cas de non-respect perçu des droits liés à la protection des renseignements personnels, une plainte peut être déposée auprès de la personne responsable de la protection des renseignements personnels ou auprès de la Commission d'accès à l'information du Québec.

Exercice des droits

Toute demande d'accès, de rectification ou de retrait du consentement doit être transmise par écrit à la personne responsable de la protection des renseignements personnels, aux coordonnées suivantes :

Responsable de la protection des renseignements personnels
rh@macpek.com
418-659-1144
2970, avenue Watt
Québec (Québec)
G1X 4P7