Politique de confidentialité et de protection des données personnelles

Adoption

La présente politique s'applique depuis le 22 septembre 2023. Elle a été révisée par le Conseil d'administration le 8 novembre 2023.

Révision

Une révision de la politique est prévue au minimum tous les deux ans. Le prochain exercice de révision est prévu, au plus tard, pour le 1er octobre 2025.

5800 rue Saint-Denis (local 602)
Montréal, H2S 3L5
(514) 382-0310

www.pair-services.org
info@pair-services.org

@PAIRservices
@pair-services

TABLE DES MATIÈRES

1. PRÉSENTATION DE LA POLITIQUE

Merci de prendre connaissance de la *Politique de confidentialité et de protection des données personnelles* de Pair.

Le respect de la vie privée ainsi que la protection des renseignements personnels sont essentiels, c'est pourquoi Pair s'engage à protéger ceux-ci conformément aux lois en vigueur. Dans cet esprit, Pair a élaboré la *Politique de confidentialité et de protection des données personnelles* qui présente les principes et procédures suivis pour garantir la confidentialité et la sécurité des données collectées. Pair s'engage à se conformer aux obligations légales en matière de confidentialité et de protection des données personnelles, notamment celles de la Loi 25, par le biais d'une liste de contrôle.

En établissant un lien d'emploi ou d'affaires ou encore en utilisant nos systèmes ou nos services, vous reconnaissez avoir lu et compris la présente politique et consentez à ce que vos données et renseignements personnels soient traités en conformité avec cette dernière, le cas échéant.

N'hésitez pas à contacter la personne responsable désignée chez Pair pour toutes questions.

2. PERSONNE RESPONSABLE DÉSIGNÉE

La personne responsable de la protection des renseignements personnels pour Pair est M. Julien Deschamps Jolin, directeur du volet rayonnement et membre du conseil d'administration. Le rôle du responsable désigné est précisé à l'annexe 1. Il peut être rejoint aux coordonnées suivantes : julien@pair-services.org — 514 382-0310, poste 503

3. DÉFINITIONS

Les définitions à considérer pour l'application de la politique, pouvant être complétées par tout autre règlement, politique, directive ou procédure y faisant référence, sont les suivantes :

Renseignement personnel :

Tout renseignement qui concerne une personne physique et qui permet de l'identifier. Le nom d'une personne, pris isolément, n'est pas un renseignement personnel. Cependant, lorsque ce nom est associé ou jumelé à un autre renseignement visant cette même personne, il devient alors un renseignement personnel.

Voici des exemples de renseignement personnel :

Le nom d'une personne et

- Date de naissance ;
- Son numéro d'assurance sociale ;
- Son numéro de carte de crédit ;
- Son numéro d'assurance maladie ;
- Ses renseignements de nature médicale ou financière ;
- Son numéro de téléphone personnel ;
- Son adresse de domicile.

Renseignement personnel sensible :

Un renseignement personnel est considéré comme sensible lorsque, par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de respect de la vie privée.

Il peut s'agir, par exemple, de renseignements médicaux, biométriques, génétiques ou financiers, ou de renseignements sur l'origine ethnique, la conviction politique, la vie ou l'orientation sexuelle, les convictions religieuses.

Incident de confidentialité :

Accès, utilisation, communication d'un renseignement personnel non autorisé par la loi, de même que sa perte ou toute autre forme d'atteinte à sa protection.

En voici quelques exemples :

- Un membre du personnel consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions ;
- Un pirate informatique s'infiltre dans un système ;

- Une personne utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne ;
- Une communication est effectuée par erreur à la mauvaise personne ;
- Une personne perd ou se fait voler des documents contenant des renseignements personnels ;
- Une personne s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer.

4. COLLECTION ET UTILISATION DES RENSEIGNEMENTS PERSONNELS

Pair ne collecte que les renseignements personnels nécessaires pour assurer ses opérations courantes dans le cadre de ses activités de consultation, de ses activités de production multimédia et de ses activités administratives. Les informations personnelles collectées peuvent inclure, sans s'y limiter :

- Nom et prénom ;
- Adresse postale ;
- Adresse électronique ;
- Numéro de téléphone ;
- Date de naissance ;
- Numéro d'assurance sociale ;
- Images et son ;
- Informations financières (relevés bancaires, informations fiscales, etc.) ;
- Autres informations pertinentes pour les activités de Pair, selon les besoins.

Pair utilise notamment les informations personnelles collectées aux fins suivantes :

- Prestation des services et des produits
- Transaction commerciale
- Gestion des dossiers des clients, des fournisseurs et partenaires
- Traitement des demandes de services
- Évaluation, amélioration et développement des services et produits
- Publicité et communications promotionnelles
- Relation d'emploi (dotation en personnel, administration de la paye et des avantages sociaux)
- Conformité aux obligations légales et réglementaires

5. MODALITÉS DE RECUEIL DU CONSENTEMENT

Pair s'engage à obtenir le consentement des personnes concernées avant de collecter, d'utiliser ou de divulguer leurs informations personnelles, sauf si la loi l'autorise ou l'exige autrement. Le consentement peut être donné de manière expresse (par exemple, en signant un formulaire) ou implicite (par exemple, en fournissant des informations volontairement).

Les personnes concernées ont le droit de retirer leur consentement à tout moment, sous réserve des restrictions légales ou contractuelles et d'un préavis raisonnable. Si une personne retire son consentement, Pair informera cette personne des conséquences de ce retrait, notamment de l'impact sur les services et les avantages qu'elle peut recevoir de Pair.

6. SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS

Pair prend des mesures de sécurité pour protéger les renseignements personnels contre la perte, le vol, l'utilisation abusive, la divulgation non autorisée et l'altération. Ces mesures incluent :

- Veille : établissement d'un registre des renseignement personnels recueillis permettant de s'assurer de ne recueillir que les renseignements nécessaires, d'évaluer leur traitement et de prévenir les risques.
- Barrières physiques et techniques : protection des locaux où sont stockés les renseignements personnels, restriction de l'accès aux zones où les renseignements personnels sont conservés, utilisation d'un pare-feu (firewall) et de logiciels antivirus.
- Procédures de sauvegarde et de restauration : protection contre les pertes accidentelles de renseignements personnels grâce à des systèmes de sauvegarde et de récupération des données.
- Gestion des accès : mise en place de procédures pour garantir que seules les personnes autorisées peuvent accéder aux renseignements personnels.
- Sensibilisation et formation du personnel : sensibilisation du personnel à l'importance de la confidentialité et formation pour la mise en place de politiques et procédures garantissant la protection des renseignements personnels.
- Gestion des incidents : mise en place de procédures pour gérer les situations d'urgence et les incidents de sécurité (se référer à l'annexe 2).
- Gestion des fournisseurs : mise en place de procédures pour s'assurer que les fournisseurs ayant accès aux renseignements personnels respectent les pratiques de confidentialité appropriées. À noter que, si un tiers fournisseur ou une autre entité à qui nous divulguons des renseignements personnels conformément à la présente Politique est situé à l'extérieur du pays, les renseignements personnels peuvent être assujettis aux lois locales des pays ou territoires où ils sont situés. Les autorités gouvernementales et les autorités chargées de l'application de la loi de ces pays ou territoires peuvent y avoir accès. Pair s'engage à retenir les services d'entreprises renommées dans des pays jugés « sûrs » conformément aux recommandations du gouvernement canadien.

Pair s'efforce de maintenir la sécurité des renseignements personnels à jour et d'évaluer régulièrement les risques pour la confidentialité des informations. Il est important de noter que, bien que Pair s'efforce de protéger les renseignements personnels, aucune méthode de transmission ou de stockage électronique n'est totalement infaillible. Par conséquent, Pair ne peut garantir une sécurité absolue des renseignements personnels, mais s'engage à prendre des mesures raisonnables pour en assurer la protection.

7. PARTAGE DES RENSEIGNEMENTS PERSONNELS

Les renseignements personnels collectés par Pair ne sont divulgués qu'aux fournisseurs et partenaires autorisés qui ont besoin d'avoir accès aux renseignements pour les fins énumérées à la présente politique et dans les limites de celle-ci, ainsi que dans les cas suivants :

- Avec le consentement de la personne concernée ;
- Pour le stockage dans des serveurs infonuagiques, dans quel cas les renseignements personnels pourraient transiter par des juridictions tierces. ;
- Pour la sécurité de l'entreprise si Pair estime qu'une telle divulgation est nécessaire pour protéger ses intérêts liés à la sécurité et la prévention des activités illégales ou nuisibles ;
- Pour la sauvegarde des intérêts vitaux d'une personne ;
- Pour la fusion ou la vente de l'entreprise ;
- Pour se conformer aux lois et règlements en vigueur.

8. CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

La durée de conservation des données collectées peut varier en fonction de leur nature et de leur utilité dans l'offre des produits et services de Pair. Une fois que les renseignements personnels ne sont plus nécessaires pour réaliser les objectifs pour lesquels ils ont été collectés, ils sont détruits de manière sécurisée et définitive.

9. TÉMOINS DE NAVIGATION, TECHNOLOGIES SIMILAIRES ET LIENS VERS D'AUTRES SITES

Pair peut utiliser des fichiers témoins (« cookies »), des balises Internet, des pixels invisibles, des fichiers journaux ou autres technologies pour collecter certains renseignements personnels relatifs aux visiteurs sur nos sites Web, ainsi que sur les destinataires de ses infolettres, invitations et autres communications.

Les témoins utilisés servent notamment à retrouver l'historique de recherche lié à la session, pour faciliter l'expérience de navigation en ligne de l'utilisateur. Il est important de savoir que, l'activation de l'option témoins peut, selon la configuration choisie, permettre à d'autres serveurs d'installer des témoins sur votre système. Vous pouvez définir les paramètres de votre navigateur pour qu'il vous informe de la présence de témoins, vous laissant ainsi la possibilité de les accepter ou non.

Veuillez noter que notre site web pourrait contenir des liens ou des renvois vers des sites de tierces parties. La présente politique cesse de s'appliquer au moment où l'utilisateur.rice quitte le site Web. Pair n'est pas responsable de la collecte ou du traitement de renseignements personnels par ces tiers ou via ces sources externes.

10. INCIDENT DE SÉCURITÉ POUR LA CONFIDENTIALITÉ DES RENSEIGNEMENTS PERSONNELS

En cas d'incident de sécurité, Pair prendra les mesures appropriées pour contenir l'incident, évaluer son impact et informer les personnes concernées conformément aux exigences légales applicables.

Toute personne avec laquelle Pair communique des renseignements personnels (employé.es, membres du conseil d'administration, fournisseurs, partenaires, sous-traitants, etc.) doit effectuer un signalement lorsqu'elle a un motif raisonnable de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel détenu par Pair. Pour ce faire, ce signalement doit être effectué sans délai à la personne responsable de la protection des renseignements personnels.

Une procédure pour la gestion d'incidents de sécurité des données est mise en place pour traiter ces situations. Se référer à l'annexe 2.

11. MODIFICATION

Pair se réserve le droit de modifier cette politique à tout moment. Les modifications apportées entreront en vigueur immédiatement après leur approbation par le conseil d'administration. Pair encourage toutes personnes intéressées à consulter régulièrement le site web de Pair pour prendre connaissance de toute modification apportée à sa politique.

12. ANNEXE 1 — RÔLE ET ENGAGEMENT DE LA PERSONNE RESPONSABLE DÉSIGNÉE

La personne responsable désignée veille à la mise en œuvre et au respect de la politique et des procédures relatives à la confidentialité et à la sécurité des informations personnelles chez Pair. Elle est chargée de traiter les questions, les préoccupations et les demandes des membres de l'organisation et des personnes concernées en matière de protection des données.

Son rôle est notamment de :

- Contribuer aux analyses de risques de sécurité de l'information afin d'identifier les menaces et les situations de vulnérabilité, s'assurer que les mesures sont prises pour assurer la sécurité des renseignements personnels conformément à la clause 4 de la politique, mettre à jour le registre des renseignements personnels, faire des recommandations à la direction générale en conséquence
- En cas d'incident de confidentialité, la personne responsable de la protection des renseignements personnels prend en charge le traitement de l'incident et s'associe avec toute autre personne utile selon la nature de l'incident (se référer à l'annexe 2)
- Remplir le formulaire, mettre à jour le registre des incidents et en tenir informé la direction générale

Par la présente, je m'engage à agir comme personne responsable désignée telle que définie dans la politique :

Julien Deschamps Jolin

8 novembre 2023

Date

13. ANNEXE 2 — PROCÉDURE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

1. Identification de l'incident

Les employé.e.s et les membres de l'organisation doivent être attentifs à toute activité suspecte ou violation potentielle de la sécurité des données. Si un incident est détecté, il doit être signalé immédiatement à la personne responsable désignée.

2. Évaluation et catégorisation de l'incident

La personne responsable désignée par cette dernière évaluera la gravité de l'incident en tenant compte des données concernées, de l'ampleur de l'incident et de l'impact potentiel sur les individus et l'organisation. L'incident sera catégorisé en fonction de sa gravité (mineur, modéré ou majeur).

3. Soutien externe

La personne désignée évaluera le besoin de soutien professionnel externe pour identifier la cause, évaluer les risques et déterminer les mesures à prendre et formulera sa recommandation à la direction générale. Le cas échéant, la direction générale prendra les mesures nécessaires pour obtenir le soutien externe nécessaire.

4. Contenir et résoudre l'incident

La personne responsable désignée, avec ou sans soutien externe, identifiera la cause, évaluera les risques et déterminera les mesures pour contenir l'incident et empêcher d'autres atteintes à la sécurité des données. Les mesures correctives appropriées seront appliquées pour résoudre l'incident et rétablir la sécurité des données.

5. Communication et notification

Si l'incident est susceptible d'avoir un impact sur la vie privée des individus concernés, la personne responsable désignée informera ces personnes des faits, des mesures prises et des mesures de protection à leur disposition. Elle peut se référer au modèle d'avis prévu à cet effet. Si nécessaire, les autorités compétentes seront également informées conformément aux exigences légales.

6. Mesures préventives et mise à jour des politiques et des procédures

En fonction des enseignements tirés de l'incident, la personne responsable désignée émet des recommandations à la direction générale. Celle-ci prend les mesures nécessaires pour réviser et mettre à jour les politiques et procédures de sécurité des données pour améliorer la protection des renseignements personnels et prévenir d'autres incidents de sécurité.

7. Formulaire et mise à jour du registre des incidents

La personne responsable désignée consignera les informations relatives à l'incident et à son traitement dans le formulaire prévu à cet effet et le déposera dans le registre des incidents.