

Politique générale de gestion des renseignements personnels

Mise à jour : 10 janvier 2024

Adoptée le : 7 février 2024

Introduction

En tant qu'organisation responsable, Développement Vaudreuil-Soulanges (DEV) accorde la plus grande attention à la protection des renseignements personnels de ses employés, clients et partenaires, en mettant en œuvre des procédures et des solutions techniques conformes aux normes de cybersécurité et aux règlements applicables, notamment la loi 25 qui modernise les dispositions législatives sur la protection des renseignements personnels au Québec.

Cette politique est publiée sur le [site Web de DEV](#) et est révisée sur une base régulière. Cette publication vise à informer les parties prenantes de la méthode de gestion et des droits relatifs à leurs renseignements personnels traités par DEV Vaudreuil-Soulanges.

Cette politique vise à définir un cadre de gouvernance pour la gestion responsable et sécurisée des renseignements personnels collectés, utilisés et conservés par DEV Vaudreuil-Soulanges. Notre engagement est de respecter les normes de protection des données, garantissant ainsi la confidentialité, l'intégrité et la disponibilité des informations personnelles en conformité avec la LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ et réglementations applicables.

La présente politique s'applique à l'ensemble du personnel, des membres, des fournisseurs et des partenaires de DEV Vaudreuil-Soulanges, ainsi qu'à toutes les données personnelles collectées auprès de nos membres, nos employés, nos fournisseurs, ou toute autre personne ayant une relation avec notre organisation.

Champ d'application

Cette politique générale s'applique à toutes les divisions et entités, sous juridiction de DEV, basées dans la province de Québec, traitant des renseignements personnels hébergés au Québec ou conservés au Québec.

Les « renseignements personnels » (RP) sont tous les renseignements qui se rapportent à une personne physique et qui permettent, directement ou indirectement, d'identifier cette personne. Cette définition s'applique aux renseignements recueillis et conservés par DEV Vaudreuil-Soulanges ou par un partenaire tiers, peu importe la nature de leur support et la forme sous laquelle ils sont accessibles.

Remarque : les renseignements personnels concernant l'exercice, par la personne concernée, d'une fonction au sein d'une entreprise (nom, titre, fonction, courriel et numéro de téléphone professionnel, etc.) ne sont pas visés par la présente politique ou la loi modernisant les dispositions législatives sur la protection des renseignements personnels au Québec

1. Gestion des renseignements personnels

1.1 Rôles et responsabilités

1.1.1 Responsable de la Protection des Renseignements Personnels (RPRP)

Le RPRP est responsable de la mise à jour et de l'application de cette politique.

Le RPRP est responsable de la protection des renseignements personnels gérés par DEV à l'interne ou communiqués à des fournisseurs ou partenaires tiers.

Le RPRP est également l'interlocuteur désigné par défaut de la Commission pour l'Accès à l'Information (CAI) du Québec.

Le RPRP est, par défaut, la personne ayant la plus haute autorité DEV.

- Adresse de correspondance : 280, boul. Harwood
Vaudreuil-Dorion (Québec) J7V 1Y5
- Nom : Brunet
- Prénom : Joanne
- Fonction : Directrice générale
- Date d'entrée dans les fonctions de RPRP : 22 septembre 2022

1.2 Prestataires informatiques

Le département TI (It-ed), notre fournisseur de services informatiques est responsable du déploiement et de la gestion des contrôles de sécurité chez DEV et il agit comme principal point de contact pour les questions de sécurité du personnel.

1.2.1 Employés et fournisseurs de services

Tout le personnel (permanent, temporaire et stagiaires) ainsi que les fournisseurs de services sont responsables de la sécurité des renseignements personnels et doivent donc comprendre et respecter cette politique et les directives connexes. Le non-respect des consignes de sécurité peut entraîner des mesures disciplinaires pour le personnel et des pénalités, recours ou terminaison de contrats pour les fournisseurs de services. Les employés et les fournisseurs de services doivent comprendre :

- Quels renseignements personnels ils utilisent, comment ils doivent être traités, stockés et transférés pour assurer leur protection;
- Quelles procédures, normes et protocoles sont en place pour l'échange des renseignements personnels avec d'autres personnes (à l'interne et à l'externe de DEV);
- Qu'ils ont la responsabilité de signaler et comment signaler un incident informatique, une tentative d'attaque (type d'hameçonnage, par exemple) ou une violation présumée de la sécurité des renseignements personnels au sein de l'organisation.

1.3 Renseignements personnels

1.3.1 Renseignements personnels recueillis

Les catégories de renseignements personnels pouvant être recueillies par DEV sont énumérées ci-dessous (liste non exhaustive) :

- **Informations d'identification** : nom, prénom, adresse postale, numéro de téléphone mobile, adresse courriel personnelle, nationalité, tranche d'âge, sexe, date de naissance, état matrimonial, photo, prix ou récompenses, historique de crédit, actifs et passifs personnels et corporatifs ainsi qu'états financiers, code postal, pays ou ville de naissance, etc.
- **Renseignements commerciaux** : historique des transactions, applications sur des programmes ou aides financières et coordonnées bancaires.
- **Renseignements sur le recrutement (employés ou programmes) et le personnel** Numéros d'assurance sociale (NAS), coordonnées bancaires, CV, antécédents scolaires, niveaux d'études, écoles, langues, expériences, lettres de recommandation, références, passe-temps, catégories d'intérêts, engagements communautaires, appartenance à des clubs ou organismes de bienfaisance (autres que politiques ou religieux), programmes éducatifs, dossiers scolaires, résultats de tests/examens, diplômes d'études secondaires, notes et moyennes pondérées cumulatives, informations d'entrevues, antécédents de crédit, etc.
- **Informations sur l'activité informatique et numérique** : adresse IP, adresse MAC, journaux, type d'appareil.
- **Cookies de navigation** : les cookies sont de petits fichiers qui peuvent être téléchargés sur l'appareil du visiteur lors de la navigation des différents sites Web de DEV. Ils permettent de reconnaître les appareils et de stocker des informations sur les préférences ou actions précédentes des utilisateurs. DEV utilise des témoins pour stocker les préférences des utilisateurs, optimiser la conception de ses sites Web ou à des fins commerciales et promotionnelles. Les cookies aident également à identifier les sections les plus populaires des sites Web de DEV et permettent de fournir un contenu qui répond plus précisément aux besoins des clients tout en améliorant leur expérience. Enfin, certains cookies de navigation sont nécessaires pour des raisons strictement techniques. Ils facilitent la navigation et augmentent la convivialité des sites Web et des applications.

- **Utilisation de Google Analytics** : Les sites de DEV utilisent Google Analytics afin de permettre l'amélioration continue. Google Analytics permet notamment d'analyser la manière dont un visiteur interagit avec un site internet de DEV. Google Analytics utilise des témoins de connexion pour générer des rapports statistiques sur le comportement des visiteurs de ces sites internet et le contenu consulté. Les informations provenant de Google Analytics ne seront jamais partagées par DEV à des tiers. Il est possible d'installer un module de navigateur complémentaire pour désactiver Google Analytics.

Les témoins de navigation servent, entre autres, à identifier les sections les plus populaires des sites Web et permettent de fournir des contenus qui répondent plus précisément aux besoins des clients tout en améliorant leur expérience. Enfin, certains témoins de navigation sont nécessaires pour des raisons strictement techniques. Ils facilitent la navigation et accroissent la convivialité des sites Web et des applications.

1.3.2 Objectifs de la collecte et du traitement des renseignements personnels

DEV recueille et traite des renseignements personnels aux fins suivantes :

- **Prospection et transactions commerciales**
 - Personnalisation des sites Web;
 - Utilisation des services offerts par DEV;
 - Gestion des transactions : facturation et paiement;
 - Envoi de communications commerciales relatives à des sociétés partenaires sélectionnées;
 - Notifications ou bulletins électroniques.
- **Recrutement (personnel et programmes)**
 - Envoi de messages sur des postes, programmes, cohortes, événements, formations et webinaires susceptibles d'intéresser les candidats;
 - Enregistrement des informations dans le cadre d'un programme subventionné et conventionné par une entente avec un tiers qui finance les activités du programme;
 - Vérification des références et des diplômes, tenue d'entrevues, organisation d'événements de recrutement, collecte d'informations sur les candidats qui ont postulé pour des offres d'emploi, identification et attraction de candidats qualifiés.
- **Analyse, recherche et développement** : optimisation des ressources informatiques, recherche et développement, notamment pour l'amélioration des sites Web, applications et expérience utilisateur, ainsi qu'à d'autres fins de recherche et d'analyse afin d'améliorer les services, activités, opérations et processus.
- **Audits, rapports et enquêtes** : statistiques, enquêtes internes, rapports sur les incidents éthiques et de conformité, gestion des conflits d'intérêts, conformité aux contrôles à l'exportation, gestion des litiges, obligations légales de l'organisation et gestion des mandats.
- **Conformité légale** : respect des obligations légales, pour répondre à une autorité, à une décision judiciaire ou à une demande de divulgation de documents.

- **Se protéger et protéger les autres** : lorsqu'il est nécessaire d'enquêter, de prévenir ou d'agir à l'égard d'activités illégales, d'escroqueries présumées, de menaces pour les personnes, de violations des politiques, des conditions ou d'autres règlements.

Les renseignements personnels ne sont utilisés qu'aux fins susmentionnées.

Les renseignements personnels peuvent également être utilisés pour une autre fin dans la mesure où cette fin reste conforme à l'objectif initial ainsi qu'aux renseignements communiqués au titulaire des renseignements personnels.

1.3.3 Cycle de vie des renseignements personnels

Conservation et mise à jour des renseignements personnels

Les renseignements personnels sont conservés aussi longtemps que nécessaire aux fins pour lesquelles ils ont été recueillis ou, au besoin, pour se conformer aux obligations légales et contractuelles de DEV.

Une procédure de mise à jour des renseignements personnels est mise en place afin d'en assurer la destruction ou l'anonymisation lorsque l'objectif est atteint.

1.3.3.1 Renseignements sur la collecte de renseignements personnels

DEV doit informer les clients et utilisateurs de la collecte de renseignements personnels de ce qui suit :

- Les fins auxquelles les renseignements sont recueillis;
- La façon dont les renseignements sont recueillis;
- Les droits d'accès et de rectification prévus par la loi;
- Le droit de retirer le consentement à la communication ou à l'utilisation des renseignements recueillis.

Cette information est communiquée :

- À travers la politique de confidentialité publiée sur les sites Web de DEV.

À travers les conditions générales et spéciales prévues lors de la conclusion d'une transaction contractuelle avec DEV. Remarque : Un renseignement personnel peut toutefois être utilisé à d'autres fins sans le consentement de la personne concernée :

- Lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli;
- Lorsque son utilisation est clairement dans l'intérêt de la personne concernée;
- Lorsque son utilisation est nécessaire à des fins d'études, de recherches ou de production de statistiques et qu'elle est dépersonnalisée.

1.3.3.2 Consentement à la divulgation de renseignements personnels

Sauf dans les cas prévus par la loi, le consentement envers l'utilisateur à la divulgation de ses renseignements personnels doit être **explicite, libre, éclairé et destiné aux fins** définies ci- dessus.

- Le consentement est recueilli au moyen d'une boîte de clique;
- Le consentement est recueilli par l'intermédiaire d'un formulaire spécifique;
- Le consentement est recueilli séparément pour chacune des fins prévues;
- Le consentement n'est valide que pour le temps nécessaire à l'atteinte des fins pour lesquelles il a été demandé.

Le consentement des mineurs de moins de 14 ans est donné par le titulaire de l'autorité parentale ou par le tuteur. Le consentement des mineurs âgés de 14 ans et plus est donné par le mineur, le titulaire de l'autorité parentale ou le tuteur.

Exemption du consentement

Le consentement à la collecte ou à la communication de RP n'est pas requis dans les cas suivants :

- Divulgence de renseignements personnels à des fins d'études, de recherches ou de production statistiques;
- Autres cas prévus par la loi : communication au Procureur, poursuite d'une infraction à une loi québécoise, application d'une convention collective, urgence avec mise en danger, etc.

1.3.3.3 Protection des renseignements personnels

DEV respecte la réglementation et les normes imposées en matière de protection des renseignements personnels et de sécurité des systèmes d'information.

Des mesures techniques, organisationnelles et opérationnelles en cas d'incidents volontaires ou involontaires pour protéger les renseignements personnels gérés par DEV, en particulier :

- Identification des renseignements personnels et des données sensibles;
- Analyse des risques liés à la gestion des renseignements personnels;
- Mesures des ressources humaines (processus d'intégration, maintien en poste, formation);
- Gouvernance de la sécurité des systèmes d'information;
- Politique sur la gestion de l'identité et les renseignements personnels;
- Moyens techniques (protection, détection, cryptage);
- Mesures de protection et rétablissement;
- Protection physique (serveurs et autres équipements informatiques).

1.3.4 Formation et sensibilisation du personnel

La formation et la sensibilisation du personnel de DEV sont des éléments clés de la protection de la vie privée.

Tous les membres du personnel sont soumis à une sensibilisation obligatoire aux risques liés aux systèmes d'information et à la protection des données personnelles.

1.3.5 Conservation et destruction

1.3.5.1 Calendrier de conservation

DEV utilise et conserve les renseignements personnels pour la durée de sa prestation de services auprès de son personnel. Les délais sont conséquents avec la prescription du calendrier de conservation de DEV, lequel est conçu en fonction des obligations légales et des meilleures pratiques.

1.3.5.2 Destruction et anonymisation

Sous réserve des délais de conservation prévus par la Loi, DEV détruit les renseignements personnels qu'il détient lorsque les fins pour lesquelles ils ont été recueillis ou utilisés sont accomplies. Lorsqu'il détruit les renseignements personnels, DEV prend les mesures nécessaires pour en assurer la confidentialité et veiller à ce qu'aucune personne non autorisée ne puisse y avoir accès pendant le processus de destruction.

DEV peut aussi anonymiser les renseignements personnels dans les cas où il entend les utiliser à des fins sérieuses et légitimes. Le cas échéant, les renseignements personnels sont anonymisés selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par la Loi.

Un renseignement est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement la personne concernée.

2. Incidents de confidentialité

Un incident de confidentialité est un événement concernant la sécurité des renseignements personnels, y compris :

- Accès, utilisation ou divulgation non autorisés de renseignements personnels;
- Perte ou autre altération de renseignements personnels.

2.1 Signalement des incidents et intervention en cas d'incident de confidentialité

Tout incident de confidentialité doit être signalé au RPRP dès que possible. Un rapport d'incident détaillé doit être établi et communiqué au RPRP dès que possible.

Tout incident qui présente un risque qu'un préjudice sérieux soit causé doit être rapidement signalé à la Commission de l'Accès à l'Information du Québec.

En outre, le RPRP doit :

- Aviser le département TI (It-ed), notre fournisseur de services informatiques et activer les plans d'intervention en cas d'incident pour arrêter la fuite et prendre les mesures nécessaires pour réduire les conséquences négatives pour les personnes concernées;

- En partenariat avec notre fournisseur de services informatiques (It-ed), mettre en place les mesures nécessaires pour éviter qu'un tel incident ne se reproduise;
- Pour préparer l'organisation aux conséquences possibles, il est recommandé de lancer une évaluation d'impact de l'incident dès que possible.

S'il y a des preuves évidentes d'une attaque malveillante, les services de police compétents devraient également en être avisés dès que possible.

2.2 Registre des incidents relatifs à la protection de la vie

Les incidents de confidentialité doivent être systématiquement consignés dans un registre des incidents de confidentialité dans lequel les rapports d'incidents signalés à la CAI seront également enregistrés.

3. Évaluation des facteurs relatifs à la vie privée (ÉFVP)

Dans certains cas, une évaluation des facteurs relatifs à la vie privée (EFVP) doit être effectuée par le RPRP en collaboration avec le gestionnaire des données concernées.

Cette démarche vise la protection des renseignements personnels et le respect de la vie privée des personnes physiques. Il s'agit d'une forme d'analyse d'impact qui se veut évolutive et, par conséquent, sera revue périodiquement.

3.1 Cas nécessitant une ÉFVP

Une ÉFVP doit être effectuée dans les cas suivants :

- Acquisition de renseignements personnels sans le consentement des personnes concernées à des fins d'études, de recherches ou de production de statistiques;
- Communication de renseignements personnels à l'extérieur du Québec;
- Avant tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant des renseignements personnels.

4. Stockage et sécurité

DEV est responsable de la protection des renseignements personnels qu'il détient. Ainsi, il veille au maintien d'un environnement sécuritaire pour assurer la confidentialité de ces renseignements.

4.1 Accès limité aux renseignements

DEV assure un accès limité aux renseignements personnels qu'il détient. Ainsi, un renseignement personnel n'est accessible, sans le consentement de la personne concernée, à toute personne qu'à la condition que ce renseignement soit nécessaire à l'exercice de ses fonctions.

4.2 Mesures de sécurité

DEV conserve tous les renseignements personnels qu'il détient sur des serveurs sécurisés situés au Québec. À cet effet, il prend les moyens techniques raisonnables pour assurer un environnement sécuritaire et protéger les renseignements personnels qu'elle détient.

Pour sa part, le personnel de DEV doit en tout temps respecter les mesures de protection.

5. Droits du propriétaire des RP et gestion des plaintes

5.1 Droits du propriétaire des renseignements personnels

Par l'entremise du responsable de la protection des renseignements personnels, DEV, traitant des renseignements personnels, doit être en mesure de répondre aux demandes suivantes :

- Retrait du consentement à l'utilisation ou à la divulgation des renseignements personnels;
- Droit d'accès et de rectification des renseignements personnels;
- Droit à l'oubli. Dans certains cas, par exemple, lorsque les renseignements personnels ne sont plus nécessaires aux fins pour lesquelles ils ont été recueillis ou que la diffusion des renseignements personnels contrevient à la loi, les renseignements personnels doivent être effacés et tous les hyperliens désindexés;
- Droit à la portabilité de l'information dans un format structuré, couramment utilisé et lisible.

5.2 Contact et gestion des plaintes relatives à la gestion de renseignements personnels

Conformément à la loi, toute personne qui souhaite avoir accès à ses renseignements personnels, qui souhaite les modifier ou qui n'est pas satisfaite du traitement de ses renseignements personnels peut communiquer avec la personne responsable des renseignements personnels chez DEV par courriel à l'adresse : vieprivee@developpementvs.com.

La procédure de demande d'accès aux renseignements personnels est gratuite pour la partie intéressée.

Les demandes d'accès aux renseignements personnels sont dûment consignées.

La transmission de tout renseignement personnel est soumise à la vérification de l'identité du demandeur selon la procédure en vigueur au sein de DEV.

Une réponse à la demande d'accès aux renseignements personnels doit être fournie au demandeur dans les 30 jours suivant la réception de la demande. Dans le cas contraire, la demande est réputée rejetée.

ANNEXES

Titre	Dernière version
Composition du comité d'accès à l'information et la protection des renseignements personnels	Février 2023

Mise à jour de la présente politique

Nous nous réservons le droit de modifier le contenu de la présente Politique de confidentialité à tout moment. Nous vous encourageons donc à la consulter régulièrement pour rester informé de la manière dont nous traitons les renseignements personnels.

Adoptée au conseil d'administration du 7 février 2024

ANNEXE 1 - Composition du comité d'accès à l'information et la protection des renseignements personnels

Titre	Prénom et nom
Directrice générale et Responsable de la protection des renseignements personnels (RPRP)	Joanne Brunet
Adjointe à la direction	Johanne Courchesne
Directrice du service aux entreprises	Marie-Eve Ménard
Coordonnatrice, services administratifs et comptabilité	Véronique Viau
Adjointe administrative - Financement	Nathalie Gagnon