INFO·TECH MONTRÉAL

LE GUIDE DU DIRECTEUR EXÉCUTIF D'ORGANISME À BUT NON LUCRATIF POUR NAVIGUER LA LOI 25

POURQUOI LA CONFORMITÉ EST IMPORTANTE

ÉVALUER VOTRE STATUT DE CONFORMITÉ ACTUEL

GESTION DES VIOLATIONS DE DONNÉES

APERÇU DE LA LOI 25

INFO·TECH MONTRÉAL

En tant qu'organisme à but non lucratif, la Loi 25 implique **de revoir et de mettre à jour vos pratiques de gestion des données.** Il s'agit de vous assurer que vous respectez les exigences de la loi tout en continuant à servir efficacement votre mission. **Les organisations qui ne se conforment pas à la Loi 25 risquent des amendes et des pénalités.**

QU'EXIGE LA LOI 25 ?

Consentement Renforcé

Les organisations doivent obtenir **un consentement clair et explicite** des individus avant de collecter leurs données personnelles.

Obligations de Transparence

Les organismes à but non lucratif doivent fournir des informations détaillées sur **la manière dont les données personnelles sont utilisées et traitées.**

Mesures de Protection des Données

La loi exige que les organisations mettent en place **des mesures de sécurité solides** pour protéger les données personnelles.

Droits des Individus

Les individus ont le droit **d'accéder, de rectifier et d'effacer** leurs données personnelles.

CONSENTEMENT RENFORCÉ

INFO·TECH MONTRÉAL

Tous les détails sur les données collectées et leur utilisation doivent être résumés clairement et en langage simple dans votre politique de confidentialité. **Ajouter une case à cocher à la fin de tous les formulaires de soumission, demandant de lire et d'accepter votre politique de confidentialité, peut aider à obtenir le consentement renforcé.**

COMMENT OBTENIR UN CONSENTEMENT RENFORCÉ ?

Consentement Éclairé

Les individus doivent être pleinement informés **de ce à quoi ils consentent**, y compris les objectifs spécifiques pour lesquels leurs données seront utilisées.

Langage Clair et Simple

Évitez le jargon juridique et assurez-vous que **les informations sont facilement compréhensibles par la personne moyenne** dans les formulaires de consentement.

Revue et Mise à Jour Régulières

Examinez et mettez régulièrement à jour les préférences de consentement pour vous assurer qu'elles restent valides. Si des changements sont apportés à l'utilisation des informations personnelles, obtenez un nouveau consentement avec les détails mis à jour.

J'ai lu et j'accepte les termes et conditions énoncés dans la politique de confidentialité.

Lien vers votre politique de confidentialité

OBLIGATIONS DE TRANSPARENCE

INFO·TECH MONTRÉAL

Votre politique de confidentialité doit inclure des détails sur les informations collectées, les objectifs pour lesquels ces informations seront utilisées et comment elles seront stockées. **Cela garantit que les utilisateurs remplissant vos formulaires sont pleinement conscients de ce à quoi ils consentent.**

QUE DOIT INCLURE MA POLITIQUE DE CONFIDENTIALITÉ ?

Informations Collectées

Essayez de limiter la collecte de données au strict minimum nécessaire à l'accomplissement de votre fonction. Il pourrait être tentant de demander le nom complet, le numéro de téléphone, l'adresse e-mail, l'adresse domiciliaire, la date de naissance, etc., mais faites un effort pour évaluer et inclure uniquement les informations nécessaires. **Cela réduit le risque de vol de données en cas de violation.**

Purpose of Collection

Reliez cela à la manière dont ces informations seront utilisées pour accomplir votre travail. Si vous communiquez exclusivement par e-mail, il peut être inutile de collecter des numéros de téléphone, et vice versa.

Coordonnées du Délégué à la Protection des Données (DPD)

Chaque organisation doit désigner un délégué à la protection des données pour superviser les pratiques de protection des données et s'assurer que les informations personnelles sont traitées conformément à la loi. **Si un DPD n'est pas explicitement désigné, la responsabilité revient à la personne occupant le poste le plus élevé, comme le directeur exécutif.**

Droits des Utilisateurs

Ces droits incluent l'accès, la correction et l'effacement de leurs informations personnelles de la base de données d'une organisation sur demande. **Les instructions pour faire de telles demandes doivent être clairement indiquées dans votre politique de confidentialité.**

INFO·TECH MONTRÉAL

MESURES DE PROTECTION DES DONNÉES

Évaluez vos pratiques de sécurité actuelles. Un audit de conformité aide à identifier les domaines où vos pratiques de gestion des données peuvent ne pas être conformes aux exigences de la Loi 25. Examinez comment vous collectez, stockez et traitez les données personnelles et évaluez si vos procédures actuelles respectent les normes légales.

OÙ DOIS-JE CHERCHER ?

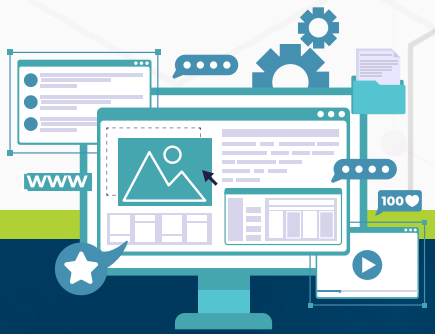
Votre site web

Auditez les sections de votre site web où vous collectez activement des données personnelles, comme les formulaires. **Gardez votre politique de confidentialité à jour** avec des informations sur la manière dont les données sont collectées, utilisées et stockées.

Où ces informations sont-elles stockées ?

Lorsque quelqu'un remplit les formulaires sur votre site, où ces informations sont-elles envoyées ?

- Sont-elles envoyées directement dans **la boîte de réception** de vous-même ou d'un autre employé ?
- Sont-elles stockées dans **un logiciel de gestion des relations avec les clients (CRM)** ?
- Sont-elles intégrées à une **feuille de calcul** existante qui se remplit lors de la soumission ?



INFO·TECH MONTRÉAL

MESURES DE PROTECTION DES DONNÉES

Une fois que vous savez où les données sont stockées, assurez-vous que **ces bases de données sont verrouillées pour empêcher tout accès non autorisé.**

COMMENT LES SÉCURISER ?

Accès Zero-trust

L'accès à ces bases de données d'informations doit être réservé **uniquement aux employés qui en ont besoin pour effectuer leur travail.** Autrement dit, si l'employé n'en a pas besoin pour accomplir sa fonction, il ne devrait pas y avoir accès.

Authentification Multi-facteurs (AMF)

Lorsqu'une personne autorisée accède à ces informations, **elle doit fournir des formes supplémentaires d'identification pour vérifier son identité.**

- Quelque chose que vous **savez** (ex. mots de passe)
- Quelque chose que vous **avez** (ex. un mot de passe à usage unique (OTP) envoyé sur votre téléphone)
- Quelque chose que vous **êtes** (ex. identifiants biométriques comme les empreintes digitales, les scans de la rétine)

CLASSEMENT DES TYPES D'AMF

INFO·TECH MONTRÉAL

Comme attacher votre vélo à un support avec des chaînes et des cadenas est probablement plus sécuritaire qu'utiliser un câble de verrouillage, **certains types de MFA sont plus sécurisés que d'autres.** Voici un aperçu des types les plus courants de MFA et de leur niveau de sécurité.

Aucune MFA, mot de passe uniquement

Il s'agit du niveau de sécurité le plus bas. Cela peut facilement être compromis par quelqu'un qui observe par-dessus l'épaule d'un utilisateur autorisé ou avec un simple enregistreur de frappe (keylogger) qui suit vos frappes. **Ne devrait jamais être utilisé pour accéder à des informations sensibles.**

Codes par courriel

Fournit une couche supplémentaire de sécurité, mais dépend de la sécurité du compte de courriel. **Si le compte de courriel est compromis et n'est pas sécurisé par l'AMF, cette méthode ne constitue plus une mesure de sécurité fiable.**

Mots de passe à usage unique (OTP) par message texte / appel

Meilleure solution que les codes par courriel, mais peut encore être rendue inefficace si un acteur malveillant parvient à faire réaffecter votre numéro de téléphone à une autre carte SIM (lire sur la fraude par échange de carte SIM).

Applications d'authentification / Jetons matériels

Génèrent des OTP à l'aide d'une application sur votre téléphone ou d'un matériel externe, **valides seulement pour une courte période** (ex. un nouveau code est généré toutes les 30 secondes).

Authentification biométrique

Utilise des caractéristiques physiques uniques comme **les empreintes digitales, les scans rétiniens ou la reconnaissance faciale.** Très sécurisée, mais peut être coûteuse à mettre en œuvre.

DROITS DES INDIVIDUS

INFO·TECH MONTRÉAL

En vertu de la Loi 25 du Québec, les utilisateurs finaux disposent de droits importants concernant leurs informations personnelles, y compris la manière dont **ils peuvent y accéder, les modifier ou les supprimer sur demande.**

QUELS SONT LES DROITS CLÉS DES UTILISATEURS ?

Droit d'être informé

Ce droit découle des obligations de transparence **exigeant que les organisations indiquent explicitement comment les informations sont collectées, utilisées et partagées.**

Droit d'accès / rectification / effacement

Les utilisateurs peuvent à tout moment demander une copie de leurs données et des informations sur la façon dont elles sont utilisées. Ils ont également le droit **de demander des corrections et de les supprimer** si les données ne sont plus nécessaires à leur objectif initial.

Droit de retirer le consentement

Les individus peuvent retirer leur consentement au traitement de leurs informations personnelles à tout moment. Cela signifie que **les organisations doivent cesser d'utiliser les données** aux fins pour lesquelles le consentement avait été initialement donné.

GESTION DES VIOLATIONS DE DONNÉES

INFO·TECH MONTRÉAL

Si vous soupçonnez qu'une violation de données a eu lieu, souvent à cause d'une infection par un logiciel malveillant, **suivez les étapes suivantes pour minimiser le risque de vol de données.**

1

MISE EN QUARANTAINE

Tous les ordinateurs que vous soupçonnez d'avoir été compromis dans une violation de données **doivent être immédiatement déconnectés du réseau** pour éviter la propagation et les dommages supplémentaires.

2

Analyse des infections

Assurez-vous que toute infection active de logiciels malveillants a été supprimée de l'appareil compromis avant de le reconnecter au réseau. Contactez votre fournisseur de services TI pour confirmer la suppression des infections.

3

Déterminer la cause

Les violations de sécurité peuvent survenir pour diverses raisons, souvent à cause d'erreurs ou d'oublis non intentionnels.

4

Prévention

Une fois la cause identifiée, concentrez-vous sur la formation des utilisateurs finaux en veillant à ce que tout le monde ait les connaissances et les outils nécessaires pour prévenir de tels incidents à l'avenir.

Une fois qu'une violation de sécurité se produit, il y a de fortes chances que certaines données aient été compromises. Bien que nous ne puissions pas changer ce qui s'est passé, nous pouvons prendre des mesures fortes pour éviter de futurs incidents et protéger nos données à l'avenir.

DES QUESTIONS ?

En tant que directeur exécutif d'un organisme à but non lucratif, rester en conformité avec la Loi 25 peut représenter un véritable défi, **notamment en matière de protection des informations personnelles, de mise en place de politiques de confidentialité rigoureuses et de mise à jour régulière des mesures de sécurité pour répondre aux exigences strictes.**

Naviguer dans ces règlements peut être complexe et chronophage, mais c'est crucial pour maintenir la confiance et la transparence avec vos donateurs et parties prenantes.

Si vous avez besoin d'aide pour rester en conformité avec la Loi 25, nous sommes à un coup de téléphone, prêts à vous soutenir à chaque étape.

INFO·TECH
MONTRÉAL

CONTACTEZ-NOUS POUR UN SOUTIEN SUPPLÉMENTAIRE

(514) 634-4636 x108 alessandro@infotechmontreal.com www.infotechmontreal.com