



Loi 25



Êtes-vous conforme ?



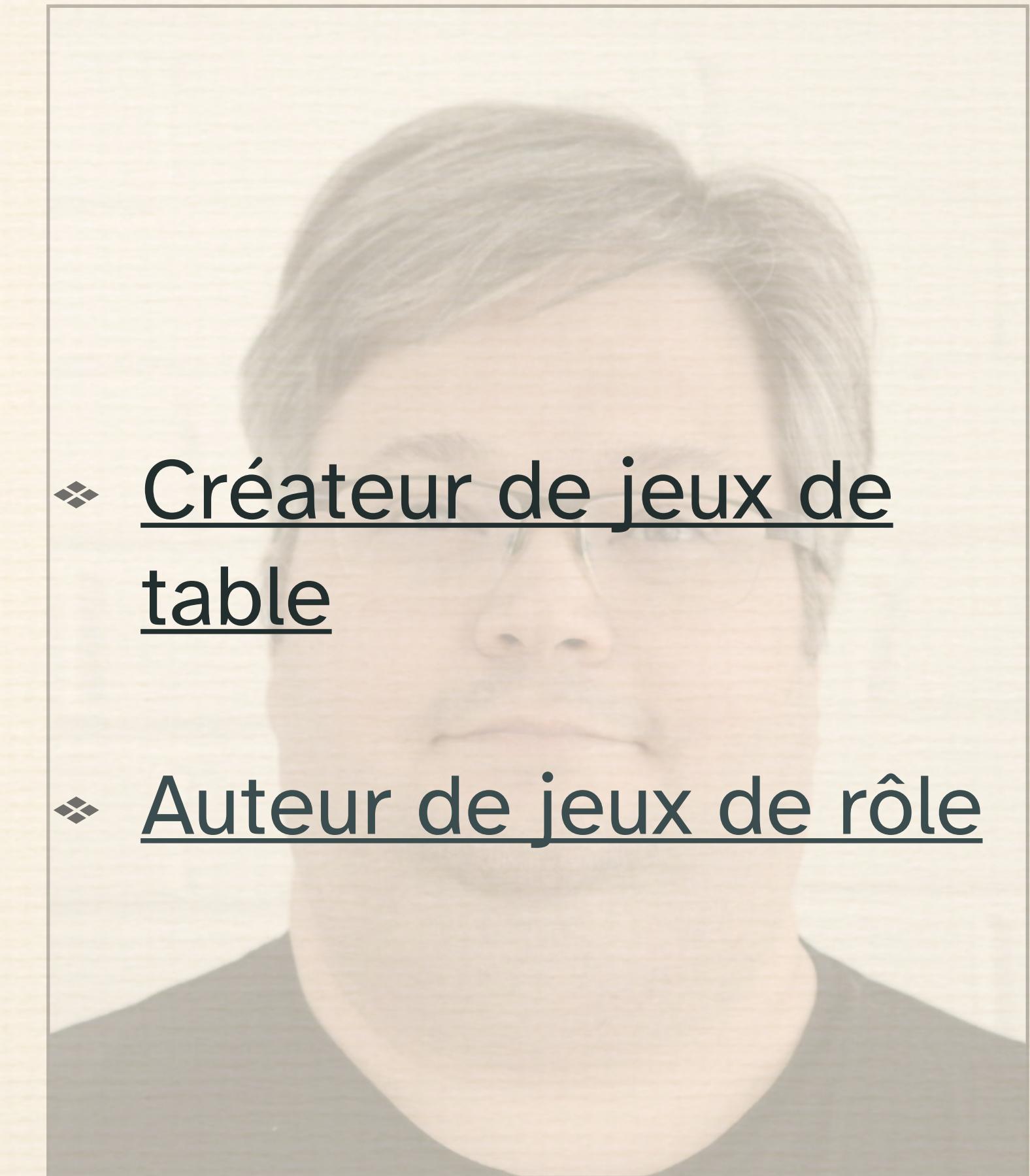
LE GNOME
ARCHIVISTE



À propos de moi

Bonjour, je m'appelle Philippe,
mentor en développement et
défense applicative.

Je suis concepteur Internet,
auteur, baladodiffuseur et
conférencier. Je me spécialise
dans le langage PHP, le cadre
d'applications Symfony, la sécurité
informatique, l'optimisation du
code et les performances.



- ❖ Créateur de jeux de table
- ❖ Auteur de jeux de rôle

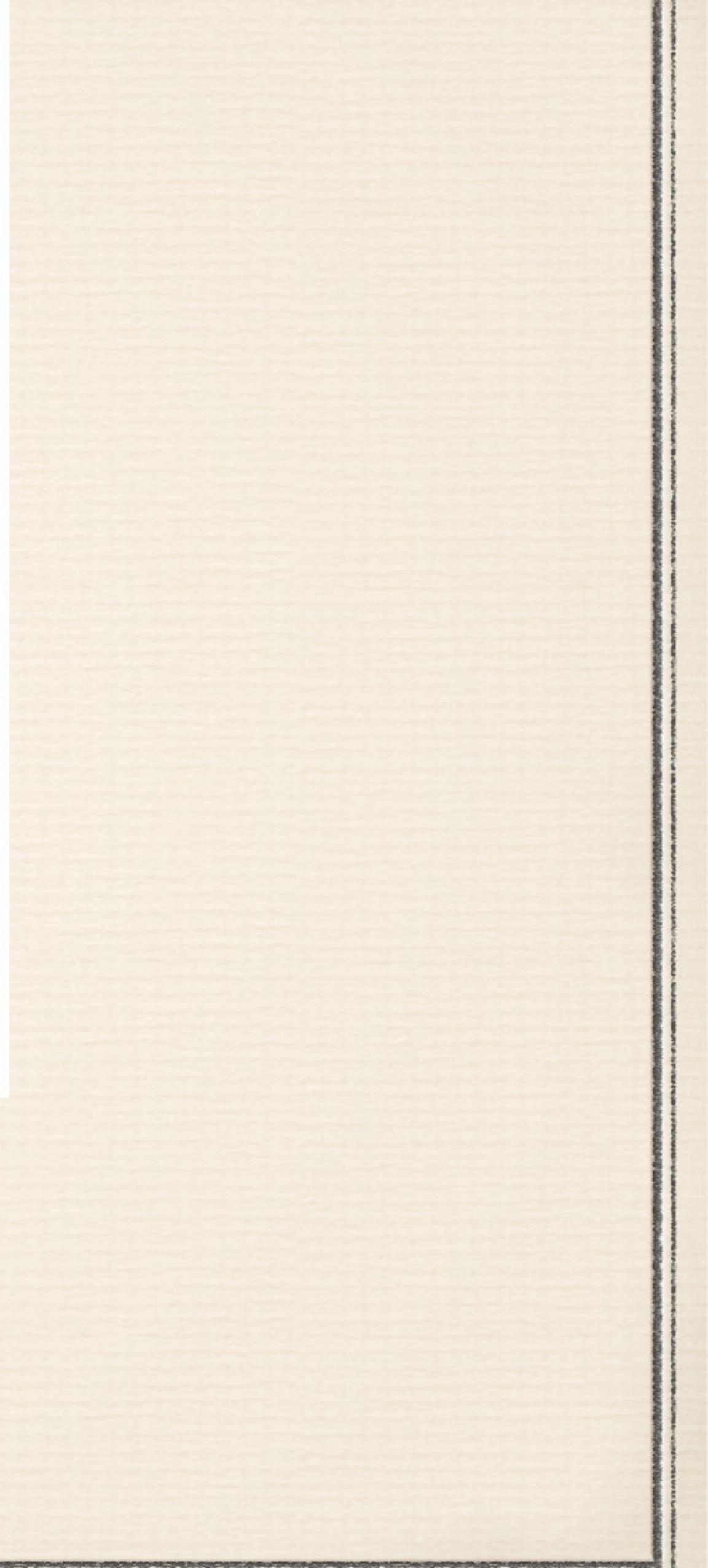


Je ne suis pas un avocat



Ne constitue pas des conseils juridiques.
Consultez plutôt vos avocats pour discuter
de votre situation particulière.





Qu'est que ça mange en hiver?

- ❖ Loi québécoise;
- ❖ Mise en place en septembre 2022;
- ❖ Protéger nos renseignements personnels;
- ❖ Assurer pour nos informations :
 - ❖ Traitement sécuritaire
 - ❖ Traitement respectueux de la vie privée.

Objectifs principaux de la Loi

- ❖ Renforcer la protection de la vie privée
- ❖ Favoriser la transparence
- ❖ Responsabiliser les entreprises
- ❖ Harmoniser le Québec avec les standards internationaux

Suis-je concerné?

- ❖ Travailleurs autonomes
- ❖ Organismes à but non lucratif
- ❖ Entreprises et compagnies
- ❖ Associations, regroupements et coopératives

Bien que je sois convaincu de ne pas collecter de données ?



VRAIMENT ?



C'est quoi des renseignements personnels ?

- ❖ Adresse courriel ;
- ❖ Identifiants numériques ;
- ❖ Numéro d'assurance sociale ;
- ❖ Adresse IP ;
- ❖ Informations bancaires ;
- ❖ Numéro de permis de conduire ;
- ❖ Adresse postale ;
- ❖ Mot de passe ;
- ❖ Poids ;
- ❖ Âge ;
- ❖ Niveau d'éducation ;
- ❖ Religion ;
- ❖ Antécédents médicaux ;
- ❖ Nom ;
- ❖ Status matrimonial ;
- ❖ Carte de crédit ;
- ❖ Numéro d'assurance-maladie ;
- ❖ Taille.
- ❖ Ethnie ;

Amende

- ❖ Entreprises individuelles ou personne physique
 - ❖ **Manquement mineur/administratif** : de 500 \$ à 50 000 \$
 - ❖ **Manquement modéré** : de 1 500 \$ à 50 000 \$
 - ❖ **Manquement grave** : de 3 000 \$ à 50 000 \$
 - ❖ **Manquement très grave** : de 5 000 \$ à 50 000 \$.

Amende

- ❖ Entreprises et organismes publiques
 - ❖ **Manquement mineur/administratif** : de 1 000 \$ à 10 \$ M ou 2 % du CA mondial de l'exercice financier précédent si ce montant est plus élevé
 - ❖ **Manquement modéré** : de 4 000 \$ à 10 \$ M ou 2 % du CA mondial de l'exercice financier précédent si ce montant est plus élevé
 - ❖ **Manquement grave** : de 8 000 \$ à 10 \$ M ou 2 % du CA mondial de l'exercice financier précédent si ce montant est plus élevé
 - ❖ **Manquement très grave** : de 15 000 \$ à 25 \$ M ou 2 à 4 % du CA mondial de l'exercice financier précédent si ce montant est plus élevé.

Que dois-je faire?

- ❖ Nommer un responsable interne de la protection des renseignements personnels, dont le rôle est clairement défini sur le site Web avec ses coordonnées.
 - ❖ La personne la plus haut placée doit assurer le respect et l'application de la loi.
 - ❖ Cette fonction peut être déléguée par écrit à une autre personne.
 - ❖ Cette personne doit approuver les politiques et pratiques de l'entreprise.
 - ❖ Cette personne doit être consultée pour toute évaluation des facteurs de la vie privée.

Que dois-je faire?

- ❖ Suite
 - ❖ Cette personne peut proposer des mesures de protection des données applicables aux projets d'acquisition, de développement ou de restructuration d'un système d'information.
 - ❖ Cette personne doit être consultée lors de l'évaluation du risque de préjudice pour une personne concernée par une violation de données.
 - ❖ Cette personne gère les demandes d'accès, de modification et de suppression.

Que dois-je faire?

- ❖ Identifiez les renseignements personnels recueillis.
- ❖ Mettre en place des règles de consentement pour la collecte, la communication et l'usage des informations personnelles.
- ❖ Concevoir un plan de gestion des incidents à appliquer en cas de violation de confidentialité.
- ❖ Ne collectez plus d'informations personnelles sur les enfants de moins de 14 ans sans le consentement parental.

Que dois-je faire?

- ❖ Établir une politique de confidentialité claire et facile à comprendre pour les utilisateurs du web. Elle doit inclure les éléments suivants :
 - ❖ Les coordonnées de votre responsable interne;
 - ❖ Les informations recueillies sur votre site Web, avec leur niveau de confidentialité;
 - ❖ À quelle(s) fin(s) collectez-vous les données;
 - ❖ La période de conservation;

Que dois-je faire?

- ❖ Suite
 - ❖ Du droit d'accès et du droit de rectification et de l'oublié ;
 - ❖ Du nom du tiers pour qui les renseignements sont recueillis ;
 - ❖ Nom des tiers ou des catégories de tiers recevant ces informations par nécessité ;
 - ❖ La possibilité de divulgation des informations hors du Québec ;
 - ❖ Comment protégez-vous ces données ?

Que dois-je faire?

- ❖ Des outils de génération de politique de confidentialité, comme celui intégré à [WordPress](#) ou le « [Générateur de Politique de Confidentialité](#) », peuvent vous aider à rédiger votre document.
- ❖ Mener une évaluation des facteurs liés à la vie privée (ÉFVP)
 - ❖ [Guide](#)
 - ❖ [Gabarit à remplir](#)



Conseils

- ❖ Assurez-vous de savoir qui possède quelles informations personnelles, internes et externes à votre entreprise.
- ❖ Il est recommandé de vérifier régulièrement les autorisations pour s'assurer que chaque personne a les autorisations appropriées. Retirez également celles accordées à un ancien employé ou prestataire.
- ❖ En cas de fuite de données, notez-les précisément et prenez des mesures adéquates. Sinon, consultez un spécialiste du web pour vous aider à trouver des solutions.

Conseils

- ❖ Pour gérer facilement vos mots de passe, utilisez un gestionnaire de mots de passe qui facilite leur création, modification et sécurité.
- ❖ Exigez des mots de passe robustes avec authentification à deux facteurs.
- ❖ Assurez-vous de donner des accès spécifiques à chaque personne concernée, plutôt que de partager les vôtres.
- ❖ Retirez les données superflues.

Conseils

- ❖ Évaluer tous les témoins (cookies) collectés par le site web et les catégoriser selon qu'ils sont :
 - ❖ **Essentiels** : nécessaires pour accéder à toutes les fonctionnalités, naviguer et assurer la sécurité. Nous utilisons également ces témoins pour vous demander votre avis et mesurer votre satisfaction.
 - ❖ **Performance** : analyse votre navigation pour y apporter des améliorations.
 - ❖ **Personnalisation** : mémorise vos préférences et adapte le contenu à votre comportement de navigation et vos choix.
 - ❖ **Publicitaires** : limitent la répétition des publicités, personnalisent les offres et services, mesurent l'efficacité des campagnes et peuvent être partagés avec des partenaires.

Conseils

- ❖ Installer une barre à témoin, c'est-à-dire une fonctionnalité qui affiche à l'utilisateur un avis indiquant la collecte de données par des témoins;
 - ❖ La barre à témoins vous permet de choisir d'accepter, de refuser ou de sélectionner des témoins.
 - ❖ La barre à témoin ne peut collecter des données personnelles qu'avec le consentement préalable de l'utilisateur.
 - ❖ Le consentement des utilisateurs doit être consigné dans un registre numérique.

Conseils

- ❖ Évaluez et vérifiez la conformité des données collectées (formulaires, commentaires, achats en ligne, etc.) avec le consentement des personnes concernées.
- ❖ Essayez d'anonymiser les données que vous collectez, sauf si c'est nécessaire.
- ❖ Établissez une durée de conservation maximale de toute information personnelle (commande clients, comptes inactifs, commentaires sur site, etc..).

Que faire lors d'une fuite de données

- ❖ Enregistrez les détails de la fuite dans un registre (papier ou numérique) et préparez-le pour une éventuelle vérification. Ce registre doit également contenir les mesures correctives.
- ❖ En cas de fuite de données, vous devez aviser la «Commission d'accès à l'information» et les personnes concernées. Mettez en avant vos efforts préventifs pour identifier la faille et les mesures prises pour assurer leur sécurité.
- ❖ Vous devrez effectuer une «évaluation des facteurs relatifs à la vie privée (EFVP)» pour identifier les risques et mettre en place des mesures préventives.



Autres lois

- ❖ Loi sur la protection des renseignements et les documents électroniques (LPRPDE) - Canada
 - ❖ Souvent appeler par la version anglophone PIPEDA
- ❖ Personal Information Protection Act (PIPA) - Alberta
- ❖ Personal Information Protection Act (PIPA) - Colombie-Britanique
- ❖ Règlement général sur la protection des données (RGPD) - Europe
- ❖ California Consumer Privacy Act

Loi 25 vs autres lois

	Loi 25	LPRPDE	PIPA-A	PIPA-CB	RGPD	CCPA
Date d'entrée en vigueur	22 septembre 2022	1er janvier 2001	1er janvier 2004	1er janvier 2004	25 mai 2018	1er janvier 2023
Autorité responsable	Commission d'accès à l'information du Québec (CAI)	Commissariat à la protection de la vie privée du Canada (CPVP)	Commissariat à l'information et à la protection de la vie privée de l'Alberta	Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique	Autorité de contrôle de chaque État membre (CNIL en France, etc.)	California Privacy Protection Agency
Champ d'application	Entités du Québec	Entreprises canadiennes sauf QC, AB, CB	Toutes les entreprises	Toutes les entreprises	Entreprises européennes ou avec clients européens	Entreprises fessants business en Californie
Renseignements personnels	Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier	Tout renseignement concernant un individu identifiable	Tout renseignement qui concerne une personne physique identifiable	Tout renseignement qui concerne une personne physique identifiable	Tout renseignement concernant une personne physique identifiée ou identifiable	Tout renseignement qui concerne une personne physique identifiable
Supports des renseignements personnels	Quel que soit le support ou la forme (écrit, graphique, sonore, visuel, informatisée ou autre)	Quels que soient leur forme ou leur support	Quels que soient leur forme ou leur support	Quels que soient leur forme ou leur support	Quel que soit le support ou le format	Quels que soient leur forme ou leur support

Loi 25 vs autres lois

	Loi 25	LPRPDE	PIPA-A	PIPA-CB	RGPD	CCPA
Renseignements anonymisés	Les renseignements sont anonymisés lorsqu'ils ne peuvent plus identifier un individu, et ce, de façon irréversible	Aucune définition pour les renseignements anonymisés	Pas de disposition précise	Pas de disposition précise	Les données personnelles anonymisées, c'est-à-dire sans possibilité d'identification de la personne concernée, ne sont pas soumises au RGPD.	Pas de disposition précise
Consentement	Il doit être évident, libre, informé et fourni pour une utilisation spécifique. Il doit être demandé à chacune de ces fins, clairement et simplement.	Il peut être explicite ou implicite, selon les circonstances et les attentes raisonnables de la personne concernée.	Peut être exprès ou tacite, chacun étant soumis à des exigences et à des limites précises	Peut être exprès ou tacite, chacun étant soumis à des exigences et à des limites précises	Le consentement doit être libre, clair, informé, non ambigu, compréhensible et limité à un objectif spécifique.	Peut être exprès ou tacite, chacun étant soumis à des exigences et à des limites précises
Enfants	Pour recueillir des informations personnelles sur un mineur de moins de 14 ans, il faut l'autorisation du représentant légal, sauf si cela profite clairement à l'enfant.	La LPRPDE ne fixe pas d'âge minimum pour le consentement des mineurs. Le CPVPC recommande l'obtention du consentement parental pour les enfants de moins de 13 ans.	Les mineurs peuvent consentir, mais doivent être assez âgés pour que leur consentement soit valable.	Les mineurs peuvent consentir, mais doivent être assez âgés pour que leur consentement soit valable.	L'âge minimum du consentement des mineurs est de 16 ans.	L'âge minimum du consentement des mineurs est de 13 ans.
Droit d'accès	Oui, sous réserve d'exceptions, telles qu'un litige ou un risque de préjudice grave pour un tiers.	Oui, sous réserve de certaines exceptions et interdictions concernant la communication	Oui, sous réserve de certaines exceptions	Oui, sous réserve de certaines exceptions	Oui, sous réserve de certaines exceptions, y compris pour des raisons juridiques ou de sécurité	Oui, sous réserve de certaines exceptions, y compris pour des raisons juridiques
Droit de corriger	Oui, si les informations sont erronées, insuffisantes ou ambiguës, ou si leur traitement est illégal.	Oui, si les renseignements sont inexacts ou incomplets	Oui, si des renseignements personnels sont erronés ou manquants.	Oui, si des renseignements personnels sont erronés ou manquants.	Oui, si les données sont inexactes ou incomplètes	Oui, si les données sont inexactes

Loi 25 vs autres lois

	Loi 25	LPRPDE	PIPA-A	PIPA-CB	RGPD	CCPA
Droit à l'effacement	Oui, pour faire cesser la diffusion des informations, supprimer ou ajouter tout lien menant à ces informations.	Non	Non	Non	Oui (sous certaines conditions)	Oui, sous réserve de certaines exceptions
Responsable de la protection de la vie privée	Voir les diapositives précédentes pour comprendre.	Obligation de désigner un responsable LPRPDE et de le communiquer.	L'organisation doit nommer un ou plusieurs responsables du respect de la PIPA.	L'organisation doit désigner un ou plusieurs responsables du respect de la PIPA de la C.-B. et fournir leurs coordonnées.	Il est obligatoire de nommer un « délégué à la protection des données » lorsque le traitement de données sensibles est effectué à grande échelle ou lorsque le suivi régulier et systématique des personnes concernées est nécessaire.	Pas de disposition précise
Transparence	Les entreprises doivent divulguer des informations claires et simples sur leurs politiques et pratiques.	Les organisations doivent rendre accessibles et compréhensibles leurs politiques de gestion des données personnelles.	Les entreprises doivent divulguer sur demande leurs politiques et pratiques de conformité, ainsi que les détails de leur utilisation de fournisseurs étrangers pour le traitement des données personnelles.	Les organisations doivent divulguer leurs politiques et pratiques de conformité à la PIPA, ainsi que leurs procédures de traitement des plaintes.	Les organisations doivent fournir à la personne concernée une grande variété d'informations lors de l'obtention des données (fins, fondements juridiques, destinataires, transfert, durée de stockage, droits, coordonnées du responsable de traitement, etc.).	Les entreprises doivent divulguer sur demande leurs politiques et pratiques de conformité, ainsi que les détails de leur utilisation et la vente des informations.
Mesures de sécurité	Les entreprises doivent mettre en œuvre des mesures de sécurité adaptées pour protéger les données personnelles, en fonction de leur sensibilité, de leur utilisation, de leur quantité, de leur répartition et du support de stockage.	Les organisations doivent prendre des mesures de sécurité adaptées au niveau de confidentialité des informations, à leur quantité, à leur localisation et à leur format, ainsi qu'à leur mode de stockage.	Les organisations doivent protéger les données contre les accès, collectes, utilisations, communications, copies, modifications, suppressions ou destructions non autorisés.	Les entreprises doivent prendre des mesures de sécurité pour prévenir les violations de données (accès, collecte, utilisation, communication, copie, modification, suppression).	Les organisations doivent prendre des mesures de sécurité adaptées au risque, y compris la pseudonymisation et le cryptage des données si nécessaire.	Les organisations doivent protéger les données contre les accès, collectes, utilisations, communications, copies, modifications, suppressions ou destructions non autorisés.
Définition d'« atteinte aux mesures de sécurité »	Une atteinte aux mesures de sécurité est une communication non autorisée, une perte de renseignements personnels ou un accès non autorisé.	Une atteinte aux mesures de sécurité est une communication non autorisée, une perte de renseignements personnels ou un accès non autorisé.	Un incident de confidentialité est une communication, une perte ou un accès non autorisé aux renseignements personnels.	Sans Objet	Une violation des données personnelles se produit lorsque des informations confidentielles sont endommagées, perdues, modifiées, divulguées ou consultées sans autorisation.	Un incident de confidentialité est une communication, une perte ou un accès non autorisé aux renseignements personnels.

Loi 25 vs autres lois

	Loi 25	LPRPDE	PIPA-A	PIPA-CB	RGPD	CCPA
Signalement d'une atteinte	Tout incident présentant un risque de préjudice sérieux doit être signalé à la CAI et aux personnes concernées.	Les signalements obligatoires concernent les atteintes présentant un « risque réel de préjudice grave ». Ils doivent être adressés au CPVP, à l'intéressé et à toute autre organisation pouvant réduire le risque.	Signalement obligatoire au CIPVP de tout accès non autorisé ou divulgation de renseignements personnels créant un « risque réel de préjudice grave ».	Aucune exigence mais signalement facultatif au CIPVP	Signalement obligatoire à l'autorité de contrôle dans les 72 heures suivant la prise de connaissance de l'incident. Informer la personne concernée sans délai lorsque la violation des données présente un risque élevé pour ses droits.	Aucune exigence
Transfert permis vers des territoires étrangers	Oui, sous réserve d'un niveau de protection équivalent pour les données personnelles. La mention dans la politique de confidentialité est requise.	Oui, sous réserve d'un niveau de protection équivalent pour les données personnelles.	Oui, sous réserve d'un niveau de protection équivalent pour les données personnelles.	Oui, mais la mention dans la politique de confidentialité est recommandée	Oui, si une « décision d'adéquation » ou d'autres garanties appropriées sont en place (clauses contractuelles, règles d'entreprise, adhésion à un code de conduite, mécanisme de certification) selon le RGPD.	Oui, mais la mention dans la politique de confidentialité est requise
Vérifications	La CAI peut, par une demande péremptoire, exiger de toute personne qu'elle fournit des informations ou des documents nécessaires à la vérification de la conformité légale.	Le CPVP peut, sur préavis, inspecter les pratiques d'une organisation en matière de gestion des données personnelles si elle a des raisons de croire qu'elle y contrevenait.	Le CIPVP peut mener une enquête pour vérifier le respect de la PIPA.	Le CIPVP peut mener une enquête pour vérifier le respect de la PIPA.	Chaque autorité de contrôle peut effectuer des audits de sécurité des données.	Procureur général ou Agence de protection de la vie privée de Californie peuvent mener une enquête pour vérifier le respect de la CCPA.
Conservation des renseignements	Aussi longtemps que nécessaire pour satisfaire aux fins prévues	Pendant le temps nécessaire pour que le demandeur d'épuiser tous les recours qu'il a en vertu de la loi	Aussi longtemps que les renseignements sont nécessaires pour des raisons juridiques ou commerciales.	Les organisations doivent détruire leurs dossiers contenant des données personnelles ou rendre impossible leur association avec une personne spécifique lorsque cela est raisonnablement possible, notamment lorsque les raisons initiales de collecte des données ne s'appliquent plus.	Pendant le temps nécessaire, en se limitant au minimum.	Aussi longtemps que les renseignements sont nécessaires pour des raisons juridiques ou commerciales.
Sanctions prévues par la loi	50 000 \$ pour une personne physique. 10M \$ ou 2 % du chiffre d'affaires mondial pour une entreprise.	Pouvant aller jusqu'à 100 000 \$ par mise en accusation	10 000 \$ pour une personne physique. 100 000 \$ pour une entreprise.	10 000 \$ pour une personne physique. 100 000 \$ pour une entreprise.	10M € ou 2 % du chiffre d'affaires mondial pour une entreprise	Jusqu'à 2 500 \$ par violation non intentionnelle Jusqu'à 7 500 \$ par violation intentionnelle ou impliquant des mineurs Action en justice avec dommages-intérêts de 100 \$ à 750 \$ par incident

Plus d'informations

❖ Gouvernement du Québec



❖ Commission d'accès à l'information



❖ Aide-Mémoire : Résumé des nouvelles obligations des entreprises



❖ Barreau du Québec : Aide-Mémoire



❖ cyber eco : Guide Pratique - Application de la loi 25



❖ Générateur de Politique de Confidentialité



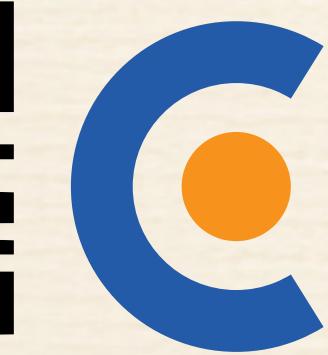
Questions ?

Si vous voulez discuter sur le sujet,
n'hésitez pas à me contacter.

 pres.loi25@ph-il.ca

 [philippegamache](https://www.linkedin.com/in/philippegamache)



 **ConFoo.ca**
DEVELOPER CONFERENCE

Vous avez 30 minutes pour
votre retour sur ConFoo.

Cette présentation a été créée avec Keynote.
L'iconographie est fournie par Keynote et Font
Awesome. La police est Atkinson Hyperlegible pour
faciliter la lecture.

Sauf sur indication contraire, toutes les
photographies sont utilisées sous licence Creative
Commons. Veuillez vous reporter à la diapositive «
crédits photo » pour plus d'informations.

Loi 25 - Êtes-vous conforme ?

Copyright © 2025 Philippe Gamache

Cette présentation est mise à disposition selon les
termes de la Licence ATTRIBUTION - PARTAGE
DANS LES MÊMES CONDITIONS 4.0
INTERNATIONAL. Pour les utilisations non couvertes
par cette licence, veuillez contacter l'auteur.



Crédits photos

- ❖ Page 4: Par spacepixelcreative via Evento
- ❖ Page 7 : Par nanoagency via Evento

Licence Evento : Payé