MÉGOPHIAS
NATATION • TROIS-RIVIÈRES

Loi 25

La loi 25 en quelques lignes

Depuis le 22 septembre 2022, toutes les entreprises du Québec, incluant les OBNL, doivent désormais être en mesure de démontrer leur conformité avec cette nouvelle réglementation. Concrètement, la Loi 25 impose aux entreprises de justifier leurs modalités de collecte, d'utilisation et de gestion des données personnelles. Attention, toutes les entreprises sont concernées par ce nouveau règlement dès qu'elles traitent des données personnelles de citoyens québécois.

Qu'est-ce que c'est que les données personnelles ?

On entend par données personnelles : « toutes les informations qui concernent directement ou indirectement un consommateur et qui sont relatives à sa vie privée, publique ou professionnelle ». Cela peut inclure un nom, des données médicales, une adresse courriel, une adresse postale, un groupe sanguin, une adresse IP, des données financières du donateur ou du bénéficiaire, etc.

Les piliers de la loi 25

La loi 25 repose sur 4 grands piliers :

- Le droit à l'oubli : Ce droit donne à toute personne concernée le droit de réclamer au responsable du traitement l'effacement des données la concernant qui ont été collectées par le responsable du traitement.
- La transparence : Ce droit permet aux personnes concernées de recevoir des informations claires sur le mode de recueil et de traitement de leurs données.
- L'obligation de notification : En cas de violation des données, les PME et OBNL doivent informer les personnes concernées et la Commission d'accès à l'information (CAI).
- Le consentement : Aucun traitement n'est possible sans consentement.

Politique de protection des renseignements personnels ou de confidentialité

1. INTRODUCTION
   1.1. OBJECTIFS La présente politique vise à :
      1.1.1. Établir les engagements qui guident les pratiques du Club de natation Mégophias du Grand Trois-Rivières inc. dans sa gestion des renseignements personnels ;
      1.1.2. Définir les rôles et les responsabilités des membres du Club de natation Mégophias du Grand Trois-Rivières inc. à l'égard des renseignements personnels et uniformiser les pratiques en la matière ;
      1.1.3. Permettre aux membres du personnel de connaître et de comprendre les exigences légales et les principes de protection des renseignements personnels dans le cadre de l'exercice de leurs fonctions.
   1.2. CHAMP D'APPLICATION
      1.2.1. La présente politique s'applique à tous les membres du personnel du Club de natation Mégophias du Grand Trois-Rivières inc. lorsqu'ils recueillent, utilisent, communiquent, conservent ou détruisent des renseignements personnels dans le cadre de leurs fonctions. Elle s'applique à tous les renseignements personnels, quel que soit leur support, de leur collecte à leur destruction.
   1.3. DÉFINITIONS
      1.3.1. Renseignement personnel: Tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier, tel que : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, l'occupation, le numéro d'assurance sociale, la date de naissance, la prise d'image et les coordonnées bancaires. Renseignement personnel sensible. Un renseignement personnel est sensible lorsque, par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'atteinte raisonnable en matière de vie privée.
      1.3.2. Renseignement anonymisé: Tout renseignement qu'il est " en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement la personne concernée".
      1.3.3. Collecte désigne le fait de recueillir, d'acquérir ou d'obtenir des renseignements personnels auprès de toute source, y compris les tierces parties, par quelque moyen que ce soit.

1.3.4. Incident de confidentialité: L'accès, l'utilisation ou la communication non autorisés par la loi d'un renseignement personnel, la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

2. **ENGAGEMENTS**

2.1. RESPONSABILITÉ: le Club de natation Mégophias du Grand Trois-Rivières inc. est responsable des renseignements personnels qu'il détient, y compris ceux dont la collecte, l'utilisation, la conservation ou la destruction est assurée par un tiers. Il met en œuvre des politiques et des pratiques qui démontrent cette responsabilité.

2.2. CONSENTEMENT: le Club de natation Mégophias du Grand Trois-Rivières inc. informe adéquatement toute personne de la collecte de renseignements qui la concernent, de l'utilisation qu'il en fera et à qui il communiquera ses renseignements à cette fin. Il s'assure d'informer la personne concernée, au plus tard au moment de la collecte :

2.2.1. du nom de l'organisme public au nom de qui la collecte est faite ;

2.2.2. des fins auxquelles ces renseignements sont recueillis ;

2.2.3. des moyens par lesquels les renseignements sont recueillis ;

2.2.4. du caractère obligatoire ou facultatif de la demande ;

2.2.5. des conséquences d'un refus de répondre ou de consentir à la demande ;

2.2.6. des droits d'accès et de rectification prévus par la loi ;

2.2.7. de la possibilité que les renseignements personnels soient communiqués à l'extérieur du Québec ou à des tiers, le cas échéant. Il obtient le consentement de la personne avant d'utiliser ou de communiquer ses renseignements à d'autres fins, à moins que la loi l'autorise à faire autrement.

2.3. LIMITATION DE LA COLLECTE: Au moment de la collecte, le Club de natation Mégophias du Grand Trois-Rivières inc. recueille uniquement les renseignements personnels nécessaires à la réalisation des fins déterminées.

3. **LIMITATION DE L'UTILISATION, DE LA COMMUNICATION ET DE LA CONSERVATION**

3.1. Le Club de natation Mégophias du Grand Trois-Rivières inc. limite l'utilisation et la communication des renseignements personnels aux seules fins auxquelles la personne concernée a été informée lors de la collecte ou à celles auxquelles elle a consenti. Elle conserve les renseignements seulement pour la durée nécessaire pour accomplir les fins déterminées.

4. **COMMUNICATION SANS LE CONSENTEMENT DE LA PERSONNE CONCERNÉE**

4.1. Le Club de natation Mégophias du Grand Trois-Rivières inc. peut divulguer certains renseignements personnels qu'il détient, sans le consentement de la personne concernée, lorsque la situation le requiert **et** que la loi le permet. Le Club de natation Mégophias du Grand Trois-Rivières inc. peut transférer des renseignements

personnels qu'il collecte à des fournisseurs de services et à d'autres tiers pour les besoins de l'organisation d'une compétition.

5. **CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS**

5.1. Le Club de natation Mégophias du Grand Trois-Rivières inc. ne conserve que les renseignements personnels qu'il détient que pour le temps nécessaire pour atteindre les fins pour lesquelles il les a collectés. Les informations sont sauvegardées par les compagnies de traitement des paiements, actuel ou futur, tels que Stripe, PayPal, Streamline sport et Qidigo pour ce qui est des informations en lien avec les données personnelles des athlètes.

6. **PROTECTION DES RENSEIGNEMENTS PERSONNELS**

6.1. Le Club de natation Mégophias du Grand Trois-Rivières inc. a mis en place des mesures de sécurité physiques, organisationnelles, contractuelles et technologiques appropriées et raisonnables afin de protéger les renseignements personnels, peu importe le support sur lequel ils sont enregistrés contre la perte ou le vol et contre l'accès, la divulgation, la copie, l'utilisation ou la modification non autorisés par la loi. Club de natation Mégophias du Grand Trois-Rivières inc. a pris des mesures pour faire en sorte que seuls les membres du personnel qui doivent absolument avoir accès à vos renseignements personnels dans le cadre de leurs fonctions soient autorisés à y accéder. Les personnes qui travaillent pour Club de natation Mégophias du Grand Trois-Rivières inc. ou en son nom doivent, notamment :

6.1.1. faire des efforts raisonnables pour minimiser le risque de divulgation non intentionnelle de renseignements personnels ;

6.1.2. prendre des précautions pour s'assurer que les renseignements personnels ne sont pas épiés, entendus, consultés ou perdus,

6.1.3. prendre des mesures raisonnables pour protéger les renseignements personnels lorsqu'elles se déplacent d'un endroit à l'autre

6.2. Identification de la personne responsable de l'application de la protection des renseignements personnels pour le Club de natation Mégophias du Grand Trois-Rivières inc.

6.2.1. Nom: Julie Desaulniers

6.2.2. Adresse: 3351 boulevard des Forges Trois-Rivières, G8Z4M3

6.2.3. Courriel: megophias@uqtr.ca

7. **PROCESSUS DE TRAITEMENT DES PLAINTES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS**

7.1. DÉPÔT D'UNE PLAINTE: Toute personne qui a des motifs de croire qu'un incident de confidentialité s'est produit et que le Club de natation Mégophias du Grand Trois-Rivières inc. a fait défaut d'assurer la confidentialité des renseignements

personnels qu'il détient peut adresser une plainte écrite auprès de la personne responsable de la protection des renseignements personnels pour demander que la situation soit corrigée. La plainte doit être formulée à megophias@uqtr.ca et comporter une description de l'incident, la date ou la période où l'incident s'est produit, la nature des renseignements personnels visés par l'incident et le nombre de personnes concernées.

8. **TRAITEMENT DE LA PLAINTE:**

8.1. Lorsqu'une plainte est reçue, la personne responsable de la protection des renseignements personnels l'analyse et la traite après en avoir accusé réception auprès de son auteur. Dans le cas où celle-ci s'avère fondée, le Club de natation Mégophias du Grand Trois-Rivières inc. prend les mesures requises pour corriger la situation dans les meilleurs délais et procède à l'inscription de l'incident au registre approprié. La personne responsable de la protection des renseignements personnels communique la réponse finale à la personne qui a formulé la plainte. La réponse finale indique notamment quelles sont les mesures de redressement qui seront appliquées.

9. **Procédure en cas d'incident de confidentialité**

9.1. Suite à la réception de la plainte, celle-ci sera analysée par la personne responsable. Celle-ci fera la vérification du fait fondé de la plainte via l'entraîneur en chef du club. Le responsable du conseil d'administration sera également mis au courant de l'incident. Selon la nature des éléments ainsi analysés, la personne responsable agira avec diligence afin d'apporter les correctifs nécessaires et avisera dans les plus brefs délais les personnes ayant été impliquées dans cette situation.

10. **Procédure de gestion des incidents de sécurité et violations des renseignements personnels**

10.1. **Aperçu :** Un plan d'intervention est essentiel pour gérer des cyberincidents de manière efficace. Dans ces moments de crise, on ne sait pas toujours comment agir et prioriser les actions. Un plan d'intervention vient réduire le stress d'oublier des aspects importants.

10.2. **Objectif :** Le but de cette procédure est de s'assurer que l'organisation est prête à intervenir en cas de cyber incident de manière à pouvoir reprendre rapidement ses activités.

10.3. **Portée :** La portée de cette procédure inclut tous les réseaux et systèmes, ainsi que les parties prenantes (clients, partenaires, employés, sous-traitants, fournisseurs) qui accèdent à ces systèmes.

10.4. **Reconnaître un cyber incident**

10.4.1. Un incident de cybersécurité peut ne pas être reconnu ou détecté immédiatement. Toutefois, certains indicateurs peuvent être les signes d'une atteinte à la sécurité, qu'un système a été compromis, d'une activité non autorisée, etc. Il faut toujours être à l'affût de tout signe indiquant qu'un incident de sécurité s'est produit ou est en cours. Certains de ces indicateurs sont décrits ci-dessous :

10.4.2. Activité excessive ou inhabituelle de la connexion et du système, notamment à partir de tout identifiant d'utilisateur (compte d'utilisateur) inactif.

10.4.3. Accès distant excessif ou inhabituel dans votre organisation. Cela peut concerner le personnel ou des fournisseurs tiers.

10.4.4. L'apparition de tout nouveau réseau sans fil (Wi-Fi) visible ou accessible.

10.4.5. Une activité inhabituelle liée à la présence de logiciels malveillants, de fichiers suspects ou de fichiers et programmes exécutables nouveaux ou non approuvés.

10.4.6. Ordinateurs ou appareils perdus, volés ou égarés qui contiennent des données de cartes de paiement, renseignements personnels ou d'autres données sensibles.

10.5. Identification de la personne responsable de l'application de la protection des renseignements personnels pour le Club de natation Mégophias du Grand Trois-Rivières inc.

Nom: Julie Desaulniers

Adresse: 3351 boulevard des Forges Trois-Rivières G8Z 4M3

Courriel: megophias@uqtr.ca

11. **Atteinte à la protection des renseignements personnels – Intervention spécifique**

11.1. S'il a été confirmé qu'un incident de sécurité lié à une atteinte à la protection des renseignements personnels s'est produit, il faudra effectuer les étapes suivantes :

11.1.1. Compléter le registre d'incidents de confidentialité pour documenter l'incident.

11.1.2. Examiner l'atteinte à la protection des renseignements personnels pour déterminer si des renseignements personnels ont été perdus en raison d'un accès ou utilisation non autorisé, d'une divulgation non autorisée ou de toute atteinte à la protection de ces renseignements personnels et qu'il existe un risque de préjudice sérieux pour les personnes concernées.

11.1.3. Dans un tel cas, le signaler à la Commission de l'accès à l'information au Québec.

11.1.4. Et, le signaler également aux personnes dont les renseignements personnels sont visés par l'incident.

12. **Rançongiciel – Intervention spécifique**

12.1. S’il a été confirmé qu'un incident de sécurité de rançongiciel s'est produit, il faudra effectuer les étapes suivantes :

12.2. Déconnecter immédiatement du réseau les appareils visés par un rançongiciel.

12.3. Ne RIEN EFFACER sur de vos appareils (ordinateurs, serveurs, etc.).

12.4. Examiner le rançongiciel et déterminer comment il a infecté l'appareil. Cela vous aidera à comprendre comment l’éliminer.

12.5. Communiquer avec les autorités locales pour signaler l'incident et coopérer à l’enquête.

12.6. Une fois le rançongiciel supprimé, une analyse complète du système doit être effectuée à l'aide d’un antivirus, d’un anti-maliciel et de tout autre logiciel de sécurité le plus récent disponible afin de confirmer qu'il a été supprimé de l'appareil.

12.7. Si le rançongiciel ne peut pas être supprimé de l'appareil (souvent le cas avec les programmes malveillants furtifs), l’appareil doit être réinitialisé au moyen des supports ou des images d'installation d'origine.

12.8. Avant de procéder à la réinitialisation à partir de supports/images de sauvegarde, vérifier qu’ils ne sont pas infectés par des maliciels. Si les données sont critiques et doivent être restaurées, mais ne peuvent être récupérées à partir de sauvegardes non affectées, rechercher les outils de déchiffrement disponibles sur nomoreransom.org. La politique est de ne pas payer la rançon, sous réserve des enjeux en cause. Il est également fortement recommandé de faire appel aux services d’un chef de projet expert en cyberattaques (breach coach). Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des rustines pour empêcher toute nouvelle attaque.

13. **Piratage de compte – Intervention spécifique**

13.1. S’il a été confirmé qu'un piratage de compte s'est produit, il faudra effectuer les étapes suivantes :

13.1.1. Aviser nos clients et fournisseurs qu’ils pourraient recevoir des courriels frauduleux de notre part, et spécifier de ne pas répondre ou cliquer sur les liens de ces courriels.

13.1.2. Vérifier si on a encore accès au compte en ligne. Sinon, communiquer avec le support de la plateforme pour tenter de récupérer l’accès.

13.1.3. Changer le mot de passe utilisé pour se connecter à la plateforme. Si le mot de passe est réutilisé ailleurs, changer également tous ces mots de passe.

13.1.4. Activer le double facteur d'authentification pour la plateforme.

13.1.5. Supprimer les connexions et les appareils non légitimes de l'historique de connexion.

14. **Perte ou vol d'un appareil – Intervention spécifique**

14.1. S'il a été confirmé qu'une perte d'équipement s'est produite, il faudra effectuer les étapes suivantes :

14.1.1. Le vol ou la perte d'un bien, tel qu'un ordinateur, un ordinateur portatif ou un appareil mobile, doit être signalé immédiatement aux autorités policières locales. Cela inclut les pertes/vols en dehors des heures d'ouverture normale et pendant les week-ends.

14.1.2. Si l'appareil perdu ou volé contenait des données sensibles et qu'il n'est pas crypté, effectuer une analyse de sensibilité, du type et du volume des données volées, y compris les numéros de cartes de paiement potentiellement concernés.

14.1.3. Dans la mesure du possible, verrouiller/désactiver les appareils mobiles perdus ou volés (p. ex. : téléphones intelligents, tablettes, ordinateurs portatifs, etc.) et procéder à un effacement des données à distance.

15. **Procédure de gestion du roulement du personnel**

15.1. **Aperçu :** Le départ d'un membre du personnel peut entraîner des dommages intentionnels, accidentels ou une perte de données. En établissant une liste de rôles et de leurs accès ainsi que d'une politique à appliquer avant un départ, vous pourrez éviter la plupart de ces pertes.

15.2. **Objectif** : Le but de cette procédure est d'établir une liste de contrôle au sein de l'organisation pour encadrer le départ d'un membre de l'équipe

15.3. **Portée :** La portée de cette procédure inclut tous les individus qui quittent l'organisation et qui possédaient des accès physiques aux appareils et systèmes de l'organisation, ou aux comptes et différentes plateformes de l'organisation.

15.4. **Procédure :** Entrevue de départ ou mise à pied

15.4.1. Éteindre les ordinateurs et appareils professionnels de l'employé.

15.4.2. Désactiver l'accès de l'employé à tous les systèmes. Suivre la liste des rôles et des accès.

15.4.3. Supprimer les données professionnelles des appareils appartenant aux employés : • Observer l'utilisateur supprimer les comptes de messagerie de son téléphone. • Une personne de l'équipe informatique peut le faire par effacement à distance, ce qui peut potentiellement supprimer des données personnelles (à utiliser avec prudence).

15.4.4. S'assurer que l'employé retourne tout équipement appartenant à l'organisation : ordinateurs portables, tablettes, clés USB, etc.

15.4.5. Compiler une liste de tous les emplacements où l'employé a stocké des données professionnelles, y compris les plateformes de stockage infonuagiques.

15.5. Téléphone

15.5.1. S'assurer que le numéro de téléphone de l'employé n'est pas transféré à un numéro externe, tel qu'un téléphone portable personnel.

15.5.2. Changer le mot de passe de la messagerie vocale.

15.5.3. Modifier le message vocal sortant conformément à vos directives de communication.

15.5.4. Désigner une personne pour surveiller la messagerie vocale jusqu'à ce que ce numéro de téléphone puisse être supprimé ou transféré à un nouvel usager..

15.6. Accès aux courriels, au Nuage et au réseau.

15.6.1. Idéalement, ne jamais supprimer le compte courriel d'un employé. La bonne pratique serait de créer une boîte courriel partagée et de bloquer les accès tels que mentionné plus bas

15.6.2. Modifier le mot de passe du compte dans le système de courriels de l'organisation. Passer en revue la section.

15.6.3. Si l'employé a utilisé un téléphone mobile personnel ou une tablette pour accéder à sa messagerie professionnelle, effacer ou supprimer le compte de messagerie si ce n'est déjà fait.

15.6.4. Créer un message d'absence pour le compte de messagerie conformément aux directives de communication de votre organisation.

15.6.5. Supprimer l'employé des listes de diffusion de courriels internes.

15.6.6. Supprimer l'employé des listes de diffusion de courriels spécialisées. S'assurer que quelqu'un d'autre est membre pour ne pas manquer ces communications.

15.6.7. Contacter les fournisseurs avec lesquels l'employé a travaillé pour les informer du départ et leur fournir un nouveau contact.

15.6.8. Désigner quelqu'un et lui donner les accès pour surveiller le courrier électronique de l'employé. Déterminer combien de temps la boîte de courriels restera disponible – 30 jours – après quoi le compte sera supprimé. S'assurer de faire un suivi après la période établie.

15.7. Accès au réseau et/ou au Nuage

15.7.1. Supprimer l'employé de tous les groupes de contrôle d'accès pour la connexion au domaine de l'organisation, RPV, bureau à distance, système d'organisation et autres systèmes.

15.7.2. Déplacer tous les fichiers de travail qui ont pu être stockés en dehors des dossiers de sauvegarde principaux de l'organisation vers un emplacement central.

15.7.3. 4.4.3 Révoquer l'accès de l'employé au compte infonuagique d'organisation.

15.7.4. 4.4.4 Supprimer les fichiers de travail de tout compte de stockage personnel.

15.7.5. 4.4.5 Passer en revue les règles d'accès au pare-feu pour confirmer que l'utilisateur ne dispose d'aucun autre accès, tel qu'un RPV direct depuis son pare-feu personnel à la maison.

15.7.6. 4.4.6 Confirmer qu'aucun logiciel d'accès à distance n'est installé sur les appareils (LogMeIn ou TeamViewer), que l'employé pourrait utiliser pour accéder à l'ordinateur ou au réseau.

16. **Liste de bonnes pratiques et outils en ligne pour la protection des renseignements personnels**

16.1. **Utilisez des mots de passe forts :** Utilisez des mots de passe comportant entre 16 et 20 caractères, composés d'une combinaison de lettres, de chiffres et de caractères spéciaux dans vos mots de passe. Évitez d'utiliser des informations personnelles évidentes et utilisez des mots de passe différents pour chaque compte.

16.2. **Gestionnaires de mots de passe** : Utilisez un gestionnaire de mots de passe tel que Dashlane, Bitwarden, NordPass, Keepass ou 1Password pour générer, stocker et gérer vos mots de passe.

16.3. **Activez l'authentification à deux facteurs** : utilisez des méthodes d'authentification à deux facteurs (2FA) lorsque cela est possible. Cela ajoute une couche de sécurité supplémentaire en demandant une deuxième preuve d'identité lors de la connexion.

16.4. **Méfiez-vous des messages suspects** : Soyez vigilant avec les courriels, les messages instantanés et les appels téléphoniques non sollicités demandant des informations personnelles. Ne cliquez pas sur les liens suspects et n'ouvrez pas les pièces jointes sources inconnues.

16.5. **Mettez à jour régulièrement vos logiciels** : Maintenez vos systèmes d'exploitation, vos applications et vos antivirus à jour en installant les dernières mises à jour et correctifs de sécurité. Les mises à jour contiennent souvent des correctifs pour les vulnérabilités connues. Une gestion proactive des mises à jour OS et matérielles limite beaucoup les risques de sécurité.

16.6. **Limitez les informations personnelles partagées en ligne** : Évitez de publier des informations personnelles sensibles, telles que votre adresse, votre numéro de téléphone ou vos détails financiers, sur les réseaux sociaux ou d'autres plateformes en ligne.

16.7. **Utilisez des réseaux Wi-Fi sécurisés :** Évitez de vous connecter à des réseaux Wi-Fi publics pour effectuer des transactions sensibles ou accéder à des informations confidentielles. Privilégiez les réseaux Wi-Fi protégés par mot de passe ou utilisez un RPV en (presque) tout temps.

16.8. **Suppression des témoins** : Utilisez les outils de nettoyage du système d'exploitation pour supprimer les témoins de suivi et les données de navigation stockées sur vos appareils

16.9. **RPV (Réseau privé virtuel)** : utilisez un RPV pour chiffrer votre connexion Internet et protéger votre vie privée en ligne. Des services populaires tels que NordLayer, ExpressVPN ou CyberGhost offrent des fonctionnalités de protection de la vie privée.

16.10. **Extensions de navigateur de confidentialité** : Installez des extensions de navigateur telles que Privacy Badger, uBlock Origin ou HTTPS Everywhere pour bloquer les traqueurs publicitaires, les publicités intrusives et forcer les connexions sécurisées.

16.11. **Chiffrement des communications** : Utilisez des services de messagerie et de communication chiffrés, tels que Signal, WhatsApp (avec le chiffrement de bout en bout activé) ou Telegram (avec le chat secret activé), pour protéger la confidentialité de vos conversations.

16.12. **Soyez prudent avec les informations de paiement en ligne** : Lorsque vous effectuez des achats en ligne, assurez-vous de le faire sur des sites sécurisés et fiables. Vérifiez la présence d'un cadenas dans la barre d'adresse et utilisez des méthodes de paiement sécurisées, telles que PayPal ou les cartes de crédit protégées.

16.13. **Chiffrement des fichiers** : Utilisez des outils de chiffrement pour protéger vos fichiers sensibles. Des logiciels tels que VeraCrypt, AxCrypt ou BitLocker vous permettent de créer des conteneurs chiffrés ou de crypter des fichiers individuels.

16.14. **Navigation privée** : Utilisez le mode de navigation privée ou incognito de votre navigateur pour limiter la collecte de données et de témoins pendant vos sessions de navigation. Cela empêche également l'enregistrement de votre historique de navigation.

16.15. **Vérification des paramètres de confidentialité** : Passez en revue et ajustez les paramètres de confidentialité de vos comptes en ligne, tels que les réseaux sociaux, les services de messagerie et les applications, pour limiter la quantité d'informations personnelles partagées et restreindre l'accès à vos données.

16.16. **Suppression des données personnelles** : Supprimez régulièrement les données personnelles inutiles ou sensibles stockées sur vos appareils, tels que les anciens courriels, les fichiers temporaires, les caches de navigateur et les historiques de recherche.

16.17. **Formation à la sensibilisation à la cybersécurité** : Familiarisez-vous avec les meilleures pratiques de cybersécurité en suivant des cours en ligne, en lisant des ressources fiables et en restant informé des dernières menaces et techniques d'attaque

17. Il est important de noter que la protection des renseignements personnels est un processus continu et qu'il est essentiel de rester vigilant et de se tenir au courant des dernières pratiques et outils de sécurité en ligne.