Politique de protection des données

Introduction

Notre politique de protection des données énonce que nous nous engageons à être responsables et à traiter les informations concernant nos employés, clients, parties intéressées et autres parties prenantes avec prudence et confidentialité absolues. Cette politique décrit comment nous collectons, conservons, manipulons et sécurisons nos données de manière équitable, transparente et confidentielle.

Cette politique garantit que PECB utilise de bonnes pratiques pour protéger les données recueillies auprès de ses clients, employés et parties prenantes. Les règles décrites dans ce document s'appliquent, que les données soient conservées électroniquement, sur papier ou sur tout autre dispositif de stockage.

1. Éléments de la politique

En tant qu'élément clé de nos activités, nous collectons et traitons toute information ou donnée qui permet d'identifier un particulier, comme le nom complet, l'adresse physique, l'adresse courriel, les photos, etc.

Cette information est recueillie uniquement avec l'entière coopération et au su des parties intéressées. Une fois que nous avons accès à cette information, les règles qui suivent s'appliquent à notre société.

Nos données seront :

- précises et constamment mises à jour ;
- collectées légitimement et dans un but clairement énoncé ;
- traitées par la société conformément à ses obligations légales et éthiques ;
- protégées par diverses mesures contre tout accès non autorisé ou illégal de parties internes ou externes.

Nos données ne seront PAS :

- communiquées de manière informelle ;
- conservées après la durée de stockage précisée ;
    - Par conséquent, les données personnelles portant sur les employés, clients et sociétés affiliées qui n'utilisent plus les services de PECB seront archivées pendant 3 ans et supprimées par la suite.
- transférées à des organismes, états ou pays qui n'adoptent pas de bonnes politiques de protection des données ;
- diffusées à quiconque sans l'approbation du propriétaire des données (sauf dans le cas de demande légitime d'un organisme d'application de la loi).

2. Rôles et responsabilités

Toute personne travaillant pour ou avec PECB est responsable de veiller à ce que la collecte, la conservation, le traitement et la protection des données soient effectués correctement. La personne-ressource responsable de la gestion du processus de protection des données est :

Personne : **Responsable de la sécurité de l'information**
Courriel : information.security@pecb.com
Téléphone : +1-844-426-7322

De plus, les titulaires des fonctions ci-dessous ont des secteurs de responsabilité clés au sein de PECB :

Le **responsable de la sécurité de l'information** et le délégué à la protection des données sont responsables de ce qui suit :

- Informer et aviser PECB en matière de protection des données et de protection de la vie privée des personnes physiques
- Surveiller la conformité en matière de protection des données et de confidentialité de PECB, et plus particulièrement à l'égard des exigences du Canada et de l'UE en matière de protection des données.
- Fournir des conseils à l'égard de l'appréciation de l'impact sur la protection des données.
- Communiquer et coopérer avec l'autorité de contrôle.
- Agir comme point de contact pour les personnes concernées à l'adresse information.security@pecb.com
- Superviser et améliorer en continu les programmes de sensibilisation à la cybersécurité et à la gestion des risques, ainsi que les améliorations connexes.
- Coopérer avec le comité de sécurité et diriger la conception, la mise en œuvre, l'exploitation et le maintien du Système de management de la sécurité de l'information conforme aux normes de la série ISO/CEI 27000.
- Veiller à ce que des essais périodiques soient effectués pour évaluer l'état de la sécurité de l'information en réalisant des revues périodiques du Système de management de la sécurité de l'information, afin de garantir la conformité aux plans de sécurité du système.
- Diriger la conception et l'exploitation des activités connexes de surveillance et d'amélioration de la conformité pour assurer le respect des politiques de sécurité internes et des lois et règlements applicables.
- Développer et gérer les mesures de contrôle permettant d'assurer la conformité avec le vaste éventail d'exigences en constante évolution résultant des normes et des règlements.

Responsable de systèmes de TI :

- Se conformer strictement à toutes les politiques de PECB relatives à la non-divulgation, à la non-concurrence et à la confidentialité de l'information.
- Rester constamment à jour à l'égard des diverses technologies et divers outils Web.
- Effectuer des mises à niveau d'équipement et logicielles des systèmes réseau et installer les correctifs de sécurité nécessaires.
- Vérifier et surveiller l'état général des réseaux et des dispositifs réseau.
- Effectuer une surveillance quotidienne du système, vérifier l'intégrité et la disponibilité de l'ensemble du matériel, des ressources du serveur, des systèmes et des processus clés, examiner les journaux de système et d'application et vérifier l'exécution des tâches planifiées.
- Mettre en œuvre, configurer et maintenir les réseaux informatiques, les logiciels et la sécurité numérique.

Service de la conformité :

- Veiller à ce que les données portant sur les détenteurs de certificats, les formateurs certifiés, les auditeurs, les examinateurs, les candidats et les surveillants soient uniquement accessibles au personnel autorisé.
- Veiller à ce que l'accès aux données portant sur les détenteurs de certificat, les formateurs, les auditeurs, les examinateurs, des candidats et les surveillants ne soit pas partagé ou donné à du personnel non autorisé.
- Veiller à la conservation appropriée et centralisée des données et des documents supplémentaires fournis par les candidats pour garantir la confidentialité, l'accessibilité et l'intégrité des données.

Service commercial :

- Veiller à ce que seul le personnel autorisé ait accès aux données portant sur les revendeurs et distributeurs autorisés de PECB.

- Veiller à ce que l'accès aux données portant sur les revendeurs et distributeurs autorisés de PECB ne soit pas partagé ou donné à du personnel non autorisé.
- Veiller à ce que l'accès aux données portant sur les listes de personnes-ressources de PECB ne soit pas partagé ou donné à du personnel non autorisé.

Administrateur système :

- Veiller à ce que l'accès aux données personnelles des utilisateurs ayant créé un compte sur le site Web de PECB soit limité au personnel autorisé seulement.
- Veiller à ce que l'accès aux données personnelles des utilisateurs ayant créé un compte sur le site Web de PECB ne soit pas partagé ou donné à du personnel non autorisé.

3. Lignes directrices générales

- L'accès aux données visées par la présente politique est limité aux seules personnes qui en ont besoin pour leur travail.
- Les données ne doivent pas être partagées de manière informelle. Lorsque l'accès à de l'information confidentielle est requis, les employés doivent le demander à leurs supérieurs hiérarchiques.
- Nous offrons une formation complète à tous les employés pour les aider à comprendre leurs responsabilités dans la manipulation des données.
- Les employés sécurisent toutes les données avec précaution et en respectant les consignes de conservation des données ci-dessous.
- En particulier, des mots de passe forts sont utilisés et ne sont jamais partagés.
- Les données personnelles ne sont pas divulguées à des personnes non autorisées, ni au sein de l'entreprise ni à l'extérieur.
- Les employés demandent l'aide de leur supérieur hiérarchique ou du responsable de la protection des données en cas de doute sur un aspect de la protection des données.

4. Stockage des données

Ces règles décrivent comment et où les données sont stockées en toute sécurité. Lorsque les données sont **stockées sur papier,** le papier doit être conservé dans un lieu sûr auquel seul le personnel autorisé peut accéder.

Ces directives s'appliquent également aux données qui sont généralement stockées électroniquement, mais qui ont été imprimées pour certaines raisons :

- le papier et les fichiers sont stockés dans un tiroir ou un classeur verrouillé ;
- les employés qui font des impressions ne laissent jamais les documents sans surveillance ;
- les impressions de données sont déchiquetées de manière sûre et détruites lorsqu'elles ne sont plus nécessaires.

Lorsque les données sont **stockées électroniquement**, elles doivent être protégées contre les accès non autorisés, les suppressions accidentelles et les menaces internes et externes.

- Les données doivent être protégées par des mots de passe forts, modifiés régulièrement et jamais partagés entre les employés.
- Si les données sont conservées sur un support amovible (comme un CD, un DVD ou un disque dur externe), le support doit être conservé en toute sécurité lorsque les données ne sont pas utilisées.
- Il est interdit, à partir du réseau d'ordinateurs de PECB, d'utiliser ou de transférer des données par l'entremise d'un CD, d'un DVD, d'un dispositif USB ou d'un disque dur externe, sauf pour les membres du personnel jouissant de droits additionnels.

- Les données doivent être stockées que sur les serveurs désignés dans les locaux de PECB et ne doivent être téléchargées que sur les services Cloud approuvés.
- L'exigence minimale pour le cryptage est AES 128 bits. Cela s'applique aux données non utilisées et lors du transport. Cela s'applique que les données soient dans les locaux ou le cloud.
- La sécurité des communications doit être prise en charge par la technologie TLS (Transport Layer Security).
- Les serveurs contenant des données personnelles doivent être situés dans un endroit sûr dont l'accès est surveillé et réservé au personnel autorisé.
- Une sauvegarde des données doit être faite quotidiennement. Les sauvegardes sont mises à l'essai régulièrement, conformément aux procédures de sauvegarde standard de la société
- Les données ne sont jamais enregistrées directement sur des ordinateurs portables ou d'autres dispositifs portables comme des tablettes, smartphones, etc.
- Tous les serveurs et ordinateurs qui contiennent des données sont protégés par le système de surveillance et le système de pare-feu.
- Toutes les données entrant dans les systèmes et le site Web de PECB sont conservées en tant que données associées à un utilisateur spécifique et des mesures sont prises pour empêcher les cas d'élévation des privilèges.
- Toutes les données entrant dans la base de données du site Web de PECB sont protégées par des certificats qui garantissent le chiffrement de la communication lors de la réception et de l'envoi d'informations.

5. Utilisation des données

- Toutes les données recueillies par PECB le sont strictement aux fins des services connexes à PECB et nécessaires à l'exhaustivité du service rendu par PECB. Aucun service sans lien avec PECB ne sera offert à partir des données collectées.
- Lorsqu'ils travaillent avec des données personnelles, les employés veillent à toujours verrouiller leur écran d'ordinateur lorsqu'un ordinateur est laissé sans surveillance.
- Les données doivent être cryptées avant d'être transférées électroniquement.
- Les employés n'enregistrent pas de copies de données personnelles sur leur propre ordinateur. L'accès et la mise à jour d'une copie visent toujours la copie centrale des données.

6. Exactitude des données et mesures à prendre

Pour garantir la protection des données, PECB prend des mesures raisonnables et s'engage à :

- restreindre et surveiller l'accès aux données sensibles et conserver les données dans le moins de lieux possible ;
- établir des procédures efficaces de collecte de données ;
- offrir aux employés des formations portant sur la protection de la vie privée et les mesures de sécurité en ligne ;
- créer un réseau sécurisé pour protéger les données en ligne contre les cyberattaques ;
- établir des procédures claires pour signaler les atteintes à la vie privée ou une utilisation malveillante des données ;
- utiliser des clauses contractuelles ou communiquer des déclarations sur la façon dont nous traitons les données ;
- mettre à jour les données, continuellement et en cas d'erreur ;
- veiller à ce que les bases de données marketing soient vérifiées par rapport aux dossiers de suppression de l'industrie ;
- installer des journaux de suivi pour surveiller les activités des employés afin de veiller à ce que les données ne soient pas utilisées à mauvais escient ;
- installer un pare-feu et un logiciel de protection qui empêchent les employés de partager et de distribuer à l'extérieur les données se trouvant sur les dispositifs de PECB, en détectant le transfert d'une grande quantité de données soit par courrier électronique, soit par l'entremise de lecteurs externes ;

- établir des pratiques de protection des données (déchiquetage de documents, verrous sécurisés, cryptage des données, sauvegardes fréquentes, autorisation d'accès, etc.).

7. Demandes d'accès d'une personne concernée

Tous les particuliers et organismes qui sont le sujet de données à caractère personnel et autres données détenues par PECB ont le droit de :

- demander **quelle information** PECB détient à leur sujet et pourquoi ;
- demander **comment accéder** à ces données ;
- savoir **comment tenir à jour** ces données ;
- savoir comment la société **se conforme à ses obligations en matière de protection des données**.

Si un particulier communique avec la société et demande cette information, il s'agit d'une demande d'accès de la personne concernée. Les demandes émanant de particuliers doivent être faites par courrier électronique au délégué à la protection des données à l'adresse suivante : information.security@pecb.com. Le responsable du traitement peut fournir un formulaire de demande standard, quoique les particuliers ne soient pas tenus de l'utiliser.

Nos clients peuvent nous envoyer directement toute demande visant ces renseignements par l'entremise d'une demande d'accès d'une personne concernée. De telles demandes peuvent être communiquées à notre délégué à la protection des données à information.security@pecb.com, ou par l'entremise du formulaire électronique accessible ici. Nous vérifierons toujours l'identité de toute personne effectuant la demande d'accès avant de transmettre toute information. Nous devrons obtenir une confirmation de la personne concernée par l'entremise de l'adresse courriel utilisée par la personne concernée pour créer son compte PECB.

La première copie des données d'une personne concernée sera fournie sans frais par le responsable du traitement des données. Cependant, des frais de 30 $ seront facturés pour toute autre copie demandée par la personne concernée. Nous nous efforcerons de fournir les données pertinentes dans un délai de 14 jours.

7.1. Modification des données

Nos clients peuvent nous demander de modifier ou de corriger les données par courriel à information.security@pecb.com ou en utilisant le formulaire électronique accessible ici. PECB vérifiera toujours l'identité de toute personne soumettant une demande d'accès de la personne concernée avant de modifier ou de corriger l'information en question.

7.2. Effacement des données

Nos clients peuvent nous demander de modifier ou de corriger les données par courriel à information.security@pecb.com ou en utilisant le formulaire électronique accessible ici. Nous fournirons de plus aux personnes concernées toute l'information nécessaire avant de procéder à l'effacement des données.

Avant que les données puissent être effacées, la personne concernée devra lire la déclaration de notre délégué à la protection des données qui explique les conséquences de l'effacement des données. Il est possible de demander l'effacement des données en tout temps.

8. Transfert transfrontalier de données

Décisions de l'Union européenne en matière d'adéquation des transferts transfrontaliers de données. Jusqu'ici, la Commission européenne a reconnu comme prestataires d'une protection adéquate Andorre,

l'Argentine, le Canada (organisations commerciales), les îles Féroé, Guernsey, Israël, l'île de Man, Jersey, la Nouvelle-Zélande, la Suisse, l'Uruguay et les États-Unis (seulement le cadre Privacy Shield). De plus, nous garantissons la protection et la confidentialité des données possédées à l'égard de personnes physiques, ce qui satisfait aux exigences juridiques. Le point de contact pour l'ensemble des autorités de protection des données (APD) et des personnes de l'UE, pour toute question ayant trait au traitement des données, est l'adresse **information.security@pecb.com.**

9. Enfants

Notre site Web n'a rien d'attrayant pour les enfants et ne s'adresse pas aux enfants de moins de 16 ans. PECB ne recueille délibérément aucune donnée personnelle nominative sur des personnes âgées de moins de 16 ans et s'efforce de respecter les exigences du Commissariat à la protection de la vie privée du Canada et du Règlement général sur la protection des données (RGPD) de l'UE. Si vous êtes parent d'un enfant de moins de 16 ans et que vous croyez que votre enfant nous a fourni des renseignements à son sujet, veuillez nous envoyer un message à l'adresse **information.security@pecb.com.**

10. Divulgation de données

Dans certaines circonstances, au besoin, PECB peut divulguer des données à des organismes d'application de la loi sans le consentement de la personne concernée. Cependant, le responsable du traitement des données vérifiera que la demande est légitime, en sollicitant l'aide du conseil d'administration et des avocats de la société, le cas échéant.

11. Politique de protection de la vie privée

Notre politique de protection de la vie privée est accessible sur notre site Web. Elle énonce quelle sera l'utilisation des données relatives aux employés, clients, parties prenantes et autres parties en cause par notre entreprise. Notre politique de protection de la vie privée se trouve ici : https://pecb.com/fr/pecb-privacy-policy