Version 2.0; Dernière mise à jour : 2026-07-20

1. Objet

PECB s'engage à protéger les données à caractère personnel de ses employés, clients, candidats à la certification/certifiés, participants aux formations, formateurs, auditeurs, surveillants, partenaires, distributeurs, sous-traitants, fournisseurs, utilisateurs du site Web et autres personnes dont elle traite les données à caractère personnel.

La présente Politique établit les principes, les responsabilités et les exigences en matière de gouvernance applicables à l'ensemble de l'organisation concernant la collecte, l'utilisation, la divulgation, le stockage, le transfert, la conservation et la suppression licites, loyaux, transparents, sécurisés et responsables des données à caractère personnel par PECB ou pour son compte.

Son objectif est de garantir que les données à caractère personnel sont traitées de manière licite, loyale, transparente et sécurisée, et conformément aux lois applicables en matière de protection des données et de la vie privée.

2. Champ d'application

La présente Politique s'applique aux éléments suivants :

- Tous les employés, dirigeants, managers, sous-traitants, consultants, travailleurs temporaires et autres personnes de PECB qui traitent des données à caractère personnel pour PECB ou pour son compte ;
- Les données à caractère personnel sous quelque forme que ce soit, y compris les informations électroniques, physiques, verbales, visuelles ou enregistrées ;
- Tous les systèmes, services, applications, plateformes, sites, environnements de travail à distance et environnements tiers approuvés de PECB ; et
- Tous les tiers qui traitent des données à caractère personnel pour le compte de PECB.

La présente Politique s'applique quel que soit le lieu où les données à caractère personnel sont consultées, stockées, transférées ou traitées.

3. Législation applicable en matière de protection des données

PECB doit se conformer à la loi singapourienne de 2012 sur la protection des données à caractère personnel (PDPA) et au Règlement (UE) 2016/679, le règlement général sur la protection des données (RGPD), y compris aux lignes directrices réglementaires applicables, chaque fois que l'un de ces cadres s'applique à une activité de traitement de données à caractère personnel. La PDPA et le RGPD doivent être considérés comme des composantes également applicables du cadre de protection des données de PECB à l'échelle de l'organisation, dans les limites de leurs champs d'application territorial et matériel respectifs.

PECB doit également se conformer aux autres lois applicables en matière de protection des données et de la vie privée dans les pays et juridictions où elle exerce ses activités ou fournit des services, ainsi qu'aux exigences contractuelles, d'accréditation et réglementaires pertinentes.

Lorsque plusieurs lois sur la protection des données s'appliquent à la même activité de traitement, PECB doit identifier et respecter les exigences applicables au titre de chaque cadre juridique pertinent. Lorsque ces exigences diffèrent ou se chevauchent, PECB doit mettre en œuvre des mesures appropriées afin de

satisfaire aux obligations applicables pertinentes et doit demander conseil au délégué à la protection des données ou au responsable juridique lorsque cela est nécessaire.

L'identité du responsable du traitement PECB concerné, ainsi que les coordonnées externes à jour du délégué à la protection des données et, le cas échéant, du représentant de PECB dans l'Union européenne, doivent être accessibles au public.

4. Définitions

Aux fins de la présente Politique, les définitions suivantes s'appliquent :

Données à caractère personnel désigne toute information se rapportant à une personne physique identifiée ou identifiable, que cette information soit exacte ou non et qu'elle soit enregistrée sous une forme matérielle ou autrement.

Traitement désigne toute opération effectuée sur des données à caractère personnel, y compris la collecte, l'enregistrement, l'organisation, la structuration, le stockage, la modification, l'extraction, la consultation, l'utilisation, la divulgation, la transmission, la limitation, la suppression, l'anonymisation ou la destruction.

Personne concernée désigne la personne physique à laquelle se rapportent les données à caractère personnel.

Responsable du traitement désigne un organisme qui détermine les finalités et les moyens du traitement des données à caractère personnel.

Sous-traitant désigne un organisme qui traite des données à caractère personnel pour le compte d'un responsable du traitement.

Intermédiaire de données désigne un organisme qui traite des données à caractère personnel pour le compte et aux fins d'un autre organisme, au sens de la PDPA de Singapour.

Consentement désigne une manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle une personne accepte le traitement de données à caractère personnel, lorsque cette norme est requise par la législation applicable.

Catégories particulières de données désigne les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques ou biométriques utilisées aux fins d'identifier une personne de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne.

Données à caractère personnel sensibles désigne les données à caractère personnel susceptibles de présenter un risque plus élevé pour la personne en cas d'accès, d'utilisation ou de divulgation inappropriés, y compris les documents d'identité, les informations financières, les identifiants de compte, les dossiers d'examen, les résultats du contrôle des sanctions et les catégories particulières de données.

Violation de données à caractère personnel désigne un incident de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données.

Anonymisation désigne le traitement de données à caractère personnel de manière que les informations ne puissent plus être associées à une personne identifiable par des moyens raisonnablement disponibles.

Pseudonymisation désigne le traitement de données à caractère personnel de manière qu'elles ne puissent plus être attribuées à une personne physique déterminée sans avoir recours à des informations supplémentaires conservées séparément et de manière sécurisée.

5. Principes de protection des données

PECB doit traiter les données à caractère personnel conformément aux principes suivants :

Licéité, loyauté et transparence - Les données à caractère personnel doivent être traitées de manière licite, loyale et d'une manière que les personnes peuvent raisonnablement comprendre.

Limitation des finalités - Les données à caractère personnel doivent être collectées, utilisées et divulguées uniquement à des fins déterminées, explicites, légitimes et raisonnables. Elles ne doivent pas être traitées à une fin incompatible, sauf si la législation applicable l'autorise.

Minimisation des données - Seules les données à caractère personnel adéquates, pertinentes et raisonnablement nécessaires à la finalité prévue doivent être collectées et traitées.

Exactitude - Des mesures raisonnables doivent être prises pour garantir que les données à caractère personnel sont exactes, complètes et, si nécessaire, tenues à jour.

Limitation de la conservation - Les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire aux fins commerciales, contractuelles, légales, réglementaires, d'accréditation, de certification, de plainte, d'appel, de sécurité ou de preuve concernées.

Intégrité et confidentialité - Les données à caractère personnel doivent être protégées au moyen de mesures techniques, physiques et organisationnelles appropriées, proportionnées à la nature, à la sensibilité et aux risques du traitement.

Responsabilité - PECB doit maintenir des politiques, procédures, enregistrements, formations, évaluations, mesures de contrôle et activités de surveillance appropriés afin de démontrer sa conformité aux exigences applicables en matière de protection des données.

6. Gouvernance et responsabilités

Tous les employés et sous-traitants de PECB partagent la responsabilité de traiter et de protéger de manière appropriée les données à caractère personnel conformément aux rôles qui leur sont attribués et aux exigences applicables de PECB.

La direction doit :

- Approuver les politiques importantes ;
- Fournir des ressources appropriées pour assurer la conformité en matière de protection de la vie privée et des données ;
- Promouvoir une culture de protection de la vie privée, de confidentialité et de responsabilité ;
- Veiller à ce que les risques importants liés à la protection de la vie privée soient pris en compte dans la prise de décision organisationnelle ;
- Soutenir l'indépendance du délégué à la protection des données ; et
- Examiner les risques importants liés à la protection de la vie privée, les incidents, les constatations d'audit et les actions correctives.

Le délégué à la protection des données doit :

- Informer et conseiller PECB et son personnel concernant les obligations en matière de protection des données ;
- Surveiller la conformité aux lois applicables en matière de protection des données, à la présente Politique et aux procédures connexes ;
- Superviser la mise en œuvre du cadre de gouvernance de PECB en matière de protection de la vie privée ;
- Fournir des conseils concernant les analyses d'impact relatives à la protection des données et les évaluations des risques liés à la protection de la vie privée ;
- Soutenir le traitement des demandes des personnes concernées ;
- Soutenir l'évaluation, la gestion et la notification des violations de données à caractère personnel ;
- Coopérer avec les autorités de contrôle et de réglementation compétentes ;
- Agir en tant que point de contact pour les autorités et les personnes concernées ;
- Soutenir les activités de formation et de sensibilisation en matière de protection de la vie privée ;
- Surveiller les actions correctives liées à la protection de la vie privée ; et
- Signaler à la direction les questions importantes relatives à la protection de la vie privée.

Le délégué à la protection des données doit être associé en temps utile aux questions impliquant un traitement important de données à caractère personnel et doit exercer son rôle avec l'indépendance, les ressources, la confidentialité et l'accès à la direction appropriés.

Le spécialiste des opérations de sécurité de l'information doit :

- Mettre en œuvre et maintenir des mesures de sécurité appropriées ;
- Réaliser des évaluations des risques liés à la sécurité de l'information ;
- Gérer les contrôles relatifs à l'identité, à l'accès, à l'authentification, au chiffrement, à la surveillance et à la sécurité des terminaux ;
- Soutenir la gestion des vulnérabilités et les tests de sécurité ;
- Soutenir l'enquête, le confinement et la remédiation des violations de données à caractère personnel ;
- Tenir à jour les enregistrements relatifs aux incidents de sécurité ; et
- Signaler les risques importants liés à la sécurité au délégué à la protection des données et à la direction.

Les managers et les responsables de processus/modules doivent :

- Identifier les données à caractère personnel traitées et la finalité de leur traitement ;
- Veiller à ce que les avis de confidentialité et les mécanismes de consentement soient mis en œuvre lorsque cela est requis ;
- Limiter l'accès aux personnes ayant un besoin professionnel autorisé ;
- Définir les exigences d'accès ;
- Approuver et examiner périodiquement les accès des utilisateurs ;
- Mettre à jour et appliquer les exigences approuvées en matière de conservation et de suppression ;
- Informer le délégué à la protection des données avant d'introduire ou de modifier de manière substantielle des activités de traitement ;
- Veiller à ce que les risques identifiés liés à la protection de la vie privée et les actions correctives soient traités.
- Soutenir la suppression sécurisée, l'anonymisation, l'exportation et la rectification des données à caractère personnel.

Les responsables de contrat chargés des relations avec des tiers doivent :

- Mener une diligence raisonnable appropriée en matière de protection de la vie privée et de sécurité ;
- Veiller à ce que les clauses contractuelles requises en matière de protection des données soient mises en œuvre ;
- Consulter le délégué à la protection des données avant de faire appel à des sous-traitants ou à des prestataires de services impliquant des données à caractère personnel importantes ;
- Veiller à ce que les données à caractère personnel soient restituées, transférées ou supprimées de manière sécurisée lorsqu'une relation de service prend fin.

Les employés et les sous-traitants doivent :

- Traiter les données à caractère personnel uniquement à des fins professionnelles autorisées ;
- Respecter la présente Politique et les procédures connexes ;
- Préserver la confidentialité ;
- Utiliser uniquement les systèmes et canaux de communication approuvés ;
- Protéger les identifiants et les droits d'accès ;
- Suivre les formations requises en matière de protection de la vie privée et de sécurité ;
- Signaler immédiatement toute violation présumée de données à caractère personnel, toute divulgation non autorisée ou toute violation de la Politique ; et
- Coopérer aux enquêtes, audits et actions correctives en matière de protection de la vie privée.

7. Fondements juridiques, consentement et traitement autorisé

Avant de traiter des données à caractère personnel, PECB doit identifier et documenter l'autorisation juridique applicable à l'activité de traitement en vertu de la législation pertinente.

PDPA de Singapour

Lorsque la PDPA de Singapour s'applique, PECB doit collecter, utiliser ou divulguer des données à caractère personnel uniquement :

- Avec le consentement de la personne ;
- Lorsque le consentement est réputé donné en vertu de la législation applicable ;
- Lorsqu'une exception autorisée au consentement s'applique ; ou
- Lorsque la loi l'autorise ou l'exige autrement.

RGPD de l'UE

Lorsque le RGPD s'applique, PECB doit identifier une base juridique appropriée, qui peut inclure :

- Le consentement de la personne concernée ;
- L'exécution d'un contrat ou de mesures précontractuelles prises à la demande de la personne concernée ;
- Le respect d'une obligation légale ;
- La sauvegarde des intérêts vitaux ;
- L'exécution d'une mission d'intérêt public, le cas échéant ; ou
- Les intérêts légitimes de PECB ou les intérêts légitimes d'un tiers, à condition que ces intérêts ne prévalent pas sur les droits et libertés de la personne concernée.

Gestion du consentement

Lorsque le consentement est requis, PECB doit s'assurer que le consentement est :

- Obtenu avant le début du traitement concerné ;
- Donné au moyen d'un langage clair et compréhensible ;
- Spécifique à la finalité concernée ;
- Séparé des conditions sans rapport, le cas échéant ;
- Susceptible d'être retiré ; et
- Modifié lorsque la finalité ou la nature du traitement change de manière substantielle.

Le retrait du consentement ne doit pas affecter le traitement déjà effectué licitement avant le retrait.

PECB peut poursuivre le traitement lorsqu'une autre base juridique, une obligation légale, une exigence contractuelle, une exigence d'accréditation ou une exception autorisée s'applique.

8. Collecte, transparence et déclaration de confidentialité

PECB doit fournir aux personnes des informations claires et accessibles sur la manière dont leurs données à caractère personnel sont traitées.

La déclaration de confidentialité doit inclure, le cas échéant :

- L'identité et les coordonnées de l'entité PECB concernée ;
- Les finalités pour lesquelles les données à caractère personnel sont traitées ;
- La base juridique ou l'autorisation juridique applicable ;
- Les catégories de données à caractère personnel traitées ;
- Les informations concernant les sous-traitants et les prestataires de services tiers ;
- Les transferts internationaux et les garanties applicables ;
- Les durées de conservation ;
- Les droits des personnes concernées et les possibilités de déposer une plainte ;

Lorsque les données à caractère personnel sont collectées directement auprès de la personne, la déclaration pertinente doit être fournie au moment de la collecte ou avant celle-ci.

9. Exigences relatives au traitement des données

9.1. Minimisation des données et exactitude

- PECB doit limiter la collecte et le traitement des données à caractère personnel à ce qui est raisonnablement nécessaire à la finalité concernée.
- PECB doit examiner périodiquement les formulaires, les champs des plateformes, les bases de données, les dossiers des employés, les dossiers d'examen et de certification, les dossiers de marketing, les dossiers d'audit et les autres référentiels contenant des données à caractère personnel.
- Les informations/enregistrements inutiles, excessifs, dupliqués ou qui ne sont plus pertinents doivent être supprimés, anonymisés ou abandonnés, selon le cas.
- PECB doit fournir des mécanismes raisonnables permettant aux personnes de consulter, mettre à jour ou rectifier leurs données à caractère personnel.

9.2. Catégories particulières de données et données à caractère personnel sensibles

PECB doit traiter les catégories particulières de données, les dossiers relatifs aux antécédents judiciaires, les informations concernant la santé, les documents d'identité, les informations financières et les autres données à caractère personnel sensibles uniquement lorsque :

- Le traitement est nécessaire à une finalité définie ;
- Une base juridique appropriée et toute condition supplémentaire requise ont été identifiées ;
- La collecte est proportionnée à la finalité ;
- L'accès est limité au personnel spécifiquement autorisé ;
- Des garanties renforcées sont appliquées ;
- La conservation est limitée ; et
- Les risques liés à la protection de la vie privée sont évalués, le cas échéant

Les données à caractère personnel sensibles ne doivent pas être collectées simplement parce qu'elles pourraient être utiles à l'avenir.

9.3. Données à caractère personnel des enfants

Les sites Web et les services de PECB ne sont pas destinés aux enfants (personnes âgées de moins de 16 ans), et PECB ne collecte pas sciemment leurs données à caractère personnel.

Lorsque PECB prend connaissance du fait que des données à caractère personnel ont été collectées auprès d'un enfant sans l'autorisation requise, des mesures raisonnables doivent être prises pour limiter l'accès aux informations, les rectifier ou les supprimer conformément à la législation applicable.

10. Protection de la vie privée dès la conception, registres et évaluation des risques

Les exigences relatives à la protection de la vie privée doivent être prises en compte lors de la conception, de l'acquisition, du développement, de la mise en œuvre ou de la modification substantielle de systèmes, services, produits, processus métiers, outils d'intelligence artificielle, activités de surveillance ou de contrôle, activités de marketing, processus relatifs aux employés et dispositifs impliquant des tiers.

Par défaut, PECB doit :

- Collecter uniquement les données à caractère personnel nécessaires ;
- Limiter l'accès en fonction du rôle et des besoins professionnels ;
- Utiliser des paramètres protégeant la vie privée ;
- Limiter la conservation ;
- Empêcher la mise à disposition sans restriction des données à caractère personnel ; et
- Appliquer des mesures de sécurité appropriées.

10.1. Inventaire des données à caractère personnel et registres des activités de traitement

PECB doit tenir à jour des registres des activités de traitement (RoPA) contenant :

- L'activité et le responsable du processus concerné ;
- Les catégories de personnes concernées et de données à caractère personnel ;

- Les finalités du traitement et la base juridique ou l'autorisation juridique applicable ;
- Les systèmes et emplacements utilisés ;
- Les destinataires et les sous-traitants ;
- Les transferts internationaux ;
- Les durées de conservation ;
- Les mesures de sécurité ;
- Les déclarations de protection de la vie privée pertinentes ;
- Le traitement automatisé.

Les responsables de processus doivent informer le délégué à la protection des données lorsqu'une activité de traitement est créée, modifiée de manière substantielle, transférée, externalisée ou abandonnée.

10.2. Évaluations des risques liés à la protection de la vie privée et analyses d'impact relatives à la protection des données

Une évaluation des risques liés à la protection de la vie privée doit être réalisée avant le début du traitement ou avant toute modification substantielle lorsque l'activité est susceptible de créer un risque important pour les personnes.

Lorsque le RGPD s'applique, une analyse d'impact relative à la protection des données doit être réalisée lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes.

Une évaluation peut être requise pour :

- La surveillance systématique ou à grande échelle ;
- Les catégories particulières de données ou l'identification biométrique ;
- L'intelligence artificielle, le profilage ou la prise de décision automatisée ;
- Le traitement concernant des personnes vulnérables ;
- Le traitement à grande échelle ; ou
- Les technologies nouvelles ou émergentes.

11. Traitement automatisé, filtrage et profilage

Lorsque PECB utilise un traitement automatisé, un filtrage, une surveillance ou un profilage, elle doit :

- Définir et documenter la finalité ;
- Identifier la base juridique applicable, le consentement/l'autorisation ;
- Informer les personnes concernées lorsque cela est requis ;
- Évaluer la qualité, la pertinence et l'exactitude des informations utilisées ;
- Mettre en œuvre des garanties contre les résultats incorrects, déloyaux ou discriminatoires ;
- Limiter l'accès aux résultats ;
- Établir des durées de conservation appropriées ;
- Prévoir une intervention humaine lorsque cela est requis ou approprié ; et
- Permettre aux personnes de remettre en question ou de contester les décisions, le cas échéant.

Pour le contrôle des listes de sanctions, PECB doit veiller à ce que les correspondances potentielles soient examinées avant toute mesure défavorable, à ce que les faux positifs soient gérés, à ce que l'accès soit limité et à ce que les résultats ne soient conservés que pendant la durée nécessaire.

PECB ne doit pas prendre de décisions fondées exclusivement sur un traitement automatisé produisant des effets juridiques ou des effets significatifs similaires, sauf si la législation applicable l'autorise et si des garanties appropriées sont mises en place.

12. Droits des personnes concernées et traitement des demandes

Les personnes peuvent exercer les droits dont elles disposent en vertu de la législation applicable. Selon la juridiction, ceux-ci peuvent inclure le droit de :

- Recevoir des informations sur le traitement ;
- Accéder aux données à caractère personnel et en obtenir une copie ;
- Rectifier les données à caractère personnel inexactes ou incomplètes ;
- Demander l'effacement ou la limitation du traitement ;
- S'opposer au traitement ;
- Recevoir les données à caractère personnel dans un format lisible ;
- Retirer son consentement ;
- Bénéficier de garanties concernant certaines décisions fondées exclusivement sur un traitement automatisé ;
- Demander une intervention humaine concernant certaines décisions automatisées ; et
- Déposer une plainte auprès d'une autorité compétente.

Ces droits ne sont pas absolus et peuvent être limités par les conditions légales applicables, les exemptions, les obligations de conservation, les exigences d'accréditation ou de certification, les actions en justice ou les droits d'autrui.

12.1. Soumission d'une demande, d'une question ou d'une plainte

Les demandes courantes visant à rectifier ou à modifier des données privées peuvent être soumises au service d'assistance clientèle de PECB à l'adresse support@pecb.com ou au moyen de l'option **Soumettre un ticket** du Centre d'aide de PECB.

Les autres demandes, suggestions ou plaintes concernant le traitement de vos données à caractère personnel doivent être adressées au délégué à la protection des données à l'adresse dpo@pecb.com.

Conformément à l'article 27 du RGPD, PECB a désigné un représentant dans l'Union européenne, établi à Lisbonne, au Portugal. Le représentant peut être contacté à l'adresse gdpr.representative@pecb.com.

12.2. Vérification, frais et délais

Les personnes peuvent exercer les droits dont elles disposent en vertu de la législation applicable.

PECB doit :

- Utiliser des mesures raisonnables et proportionnées pour vérifier l'identité et l'autorité du demandeur ;
- Éviter de demander plus de données à caractère personnel que nécessaire aux fins de la vérification ;
- Traiter les demandes gratuitement, sauf si des frais sont autorisés par la loi (*des frais sont applicables en cas de nombreuses demandes d'accès des personnes concernées (DSAR)*) ;
- Informer le demandeur à l'avance si des frais légaux s'appliquent ;
- Répondre sans retard injustifié et dans le délai légal applicable ; et

- Informer le demandeur, au cours du délai de réponse initial, si une prolongation légale est nécessaire.

12.3. Refus, limitation et effacement

Lorsqu'une demande est refusée ou limitée, PECB doit en expliquer les raisons, sous réserve des restrictions légales, et indiquer les possibilités de plainte ou d'appel disponibles.

PECB peut conserver les informations dont l'effacement a été demandé lorsque cela est nécessaire aux fins suivantes :

- Conformité légale ou réglementaire ;
- Obligations de certification ou d'accréditation ;
- Obligations contractuelles ;
- Traitement des plaintes et des appels ;
- Prévention de la fraude ;
- Actions en justice ;
- Registres relatifs à la sécurité, à l'audit, aux finances ou à la comptabilité ; ou
- Toute autre finalité licite et documentée.

Avant de supprimer un compte ou les registres connexes, PECB doit expliquer les conséquences pertinentes, y compris la perte éventuelle d'accès aux registres de certification, aux registres d'examen, aux supports de formation ou aux services.

13. Communications marketing et communications de service

Lorsque cela est requis, PECB doit obtenir le consentement avant d'envoyer des communications marketing concernant des formations, des newsletters, des webinaires, des événements, des promotions ou des services connexes.

Les destinataires doivent pouvoir retirer leur consentement ou se désabonner facilement.

PECB peut utiliser les coordonnées obtenues dans le cadre d'une relation client existante pour envoyer des communications ciblées et pertinentes, y compris des communications comportant un élément promotionnel, concernant les propres services de PECB qui sont similaires ou étroitement liés à cette relation et qui sont raisonnablement considérés comme pertinents ou importants. Ces communications peuvent être envoyées sur la base des intérêts légitimes de PECB ou d'une exception applicable concernant les clients existants, et les destinataires peuvent s'y opposer ou se désabonner à tout moment.

PECB peut envoyer les communications de service non promotionnelles nécessaires pour :

- Créer ou gérer des comptes ;
- Administrer les certifications, les formations, les examens, les demandes, les paiements ou les factures ;
- Fournir une assistance clientèle ;
- Communiquer des informations relatives à la sécurité, aux questions légales, réglementaires, d'accréditation, de politique ou contractuelles ; ou
- Informer les utilisateurs de modifications affectant des services actifs.

Les destinataires ne peuvent généralement pas refuser de recevoir les communications de service nécessaires tant que le compte, l'inscription, la certification, l'examen, le contrat ou le service concerné reste actif. Les communications de service ne doivent pas inclure de contenu promotionnel inutile.

Les partenaires indépendants de PECB peuvent traiter des données à caractère personnel et envoyer des communications conformément à leurs propres déclarations de confidentialité. PECB n'est pas responsable des activités marketing indépendantes d'un partenaire.

14. Conservation et suppression sécurisée

Les données à caractère personnel doivent être conservées conformément au calendrier de conservation approuvé de PECB.

Les durées de conservation doivent prendre en compte :

- La finalité initiale du traitement ;
- Les obligations contractuelles ;
- Les exigences de certification, d'accréditation, d'examen et de formation ;
- Les obligations légales, réglementaires, financières et comptables ;
- Les délais liés aux plaintes, aux appels, à la prescription, aux audits et aux enquêtes ;
- Les exigences en matière de prévention de la fraude ; et
- Les besoins légitimes en matière de preuve.

PECB doit examiner périodiquement les données à caractère personnel conservées.

Lorsque les informations ne sont plus nécessaires, elles doivent être supprimées de manière sécurisée, détruites, anonymisées de manière irréversible ou éliminées par une autre méthode approuvée.

Les documents papier doivent être déchiquetés ou détruits de manière sécurisée par un service approuvé de destruction confidentielle. Les enregistrements électroniques doivent être supprimés au moyen de méthodes approuvées adaptées au système et au support de stockage.

Lorsque la suppression immédiate des sauvegardes n'est pas techniquement réalisable, l'accès doit être limité et les informations ne doivent pas être restaurées ni utilisées, sauf à des fins légitimes de récupération.

La suppression peut être suspendue lorsque les informations font l'objet d'une obligation de conservation à des fins juridiques, d'une enquête, d'une plainte, d'un appel, d'un audit, d'une exigence réglementaire ou d'accréditation, ou d'une action en justice réelle ou anticipée.

15. Sécurité des données et pratiques de travail

PECB doit mettre en œuvre des mesures techniques, physiques et organisationnelles proportionnées à la nature, au volume, à la sensibilité, au contexte et aux risques liés aux données à caractère personnel traitées.

Les mesures de contrôle peuvent inclure :

- La classification des informations, le principe du moindre privilège, l'accès selon le besoin d'en connaître et la séparation des tâches ;
- Une authentification forte, l'authentification multifacteur et des revues périodiques des accès ;
- Le chiffrement des données en transit et au repos, le cas échéant ;
- Des protocoles de communication sécurisés, la journalisation, la surveillance et la prévention des pertes de données ;

- Des mesures de contrôle relatives aux terminaux, aux pare-feu, aux réseaux, aux vulnérabilités et à la gestion des correctifs ;
- Des mesures de sauvegarde sécurisée, de récupération, de continuité d'activité et de reprise après sinistre ;
- Des mesures de contrôle des accès physiques et des pratiques de bureau propre ;
- Des pratiques de développement logiciel sécurisé, des tests d'intrusion et des évaluations de sécurité ; et
- Des mécanismes approuvés de conservation et de suppression sécurisée.

15.1. Enregistrements électroniques et physiques

Les données à caractère personnel électroniques doivent être stockées et transmises uniquement au moyen de systèmes, d'appareils, de services cloud et de méthodes sécurisées approuvés. Les copies locales inutiles ne doivent pas être conservées sur des appareils personnels ou non approuvés.

Les enregistrements physiques doivent être conservés dans des zones verrouillées ou autrement sécurisées, être accessibles uniquement au personnel autorisé, être protégés pendant leur transport et être détruits de manière sécurisée lorsqu'ils ne sont plus nécessaires.

15.2. Supports amovibles

Les données à caractère personnel ne doivent pas être stockées sur des supports amovibles sans besoin professionnel documenté ni autorisation. Les supports amovibles approuvés doivent être chiffrés lorsque cela est possible, physiquement sécurisés, suivis le cas échéant et effacés ou détruits de manière sécurisée après utilisation.

15.3. Pratiques du personnel

Le personnel doit :

- Verrouiller les écrans lorsque les appareils sont laissés sans surveillance ;
- Protéger les mots de passe et les identifiants d'authentification ;
- Vérifier les destinataires avant de transmettre des données à caractère personnel ;
- Éviter les canaux de communication ou de stockage non approuvés ;
- Utiliser uniquement les applications et les emplacements de stockage autorisés ;
- Empêcher toute visualisation ou écoute non autorisée ; et
- Signaler immédiatement toute activité suspecte.

16. Sous-traitants, prestataires de services et partenaires

Avant de désigner un sous-traitant, un intermédiaire de données, un fournisseur de services cloud, un fournisseur de logiciels ou tout autre prestataire de services qui traitera des données à caractère personnel, PECB doit mener une diligence raisonnable proportionnée en matière de protection de la vie privée et de sécurité.

La diligence raisonnable doit prendre en compte :

- La nature, la sensibilité, la finalité et le volume du traitement ;
- Les lieux de traitement et de stockage ;
- Les mesures de sécurité et l'historique des violations ;
- La prise en charge des demandes des personnes concernées ; et

- Les modalités relatives aux transferts internationaux.

Les accords écrits doivent traiter, le cas échéant, des éléments suivants :

- L'objet, la durée, la nature et la finalité du traitement ;
- Les instructions documentées et la confidentialité ;
- Les exigences en matière de sécurité ;
- L'assistance concernant les demandes des personnes concernées et la gestion des violations ;
- Les droits d'audit et d'assurance ;
- Les transferts internationaux ;
- La restitution ou la suppression des données à caractère personnel ; et
- Les obligations en cas de cessation de la relation.

Les sous-traitants et les intermédiaires de données traitent les données conformément à leurs propres politiques de confidentialité.

Lorsque PECB agit en tant que sous-traitant ou intermédiaire de données, elle doit respecter le contrat concerné, les instructions documentées et la législation applicable.

Les partenaires indépendants sont responsables des activités de traitement pour lesquelles ils déterminent les finalités et les moyens. Lorsque PECB et un autre organisme déterminent conjointement ces finalités et ces moyens essentiels, leurs responsabilités doivent être documentées dans le cadre d'un accord approprié.

17. Transferts internationaux de données

Les données à caractère personnel ne doivent être transférées hors de Singapour, de l'EEE ou d'une autre juridiction d'origine que conformément à la législation applicable.

Pour les transferts depuis Singapour, PECB doit prendre des mesures appropriées pour veiller à ce que le destinataire situé à l'étranger assure un niveau de protection comparable à celui exigé par la PDPA de Singapour et le RGPD.

Les garanties autorisées peuvent inclure les suivantes :

- Des obligations contractuelles ;
- Des règles d'entreprise contraignantes ou des accords internes au groupe ;
- Des certifications reconnues par la loi ;
- Des exemptions prévues par la loi ;
- D'autres mécanismes légalement autorisés.
- Une décision d'adéquation ;
- Des clauses contractuelles types.

18. Divulgation de données à caractère personnel

PECB peut divulguer des données à caractère personnel uniquement :

- À une fin autorisée et documentée ;
- Avec un consentement valide lorsque cela est requis ;
- À un sous-traitant, un prestataire de services ou un partenaire PECB autorisé et approuvé ;
- À des organismes d'accréditation ou de certification lorsque cela est nécessaire ;

- Aux autorités compétentes ;
- Lorsque la loi, une ordonnance judiciaire ou une procédure légale l'exige ;
- Aux fins de la constatation, de l'exercice ou de la défense de droits en justice ;
- Afin de protéger les droits, les biens, la sûreté ou la sécurité de PECB ou d'autrui ; ou
- Lorsqu'une autre autorisation juridique applicable existe.

Les demandes émanant de tribunaux, d'autorités de réglementation, d'organismes chargés de l'application de la loi ou d'autorités publiques doivent faire l'objet d'un examen quant à leur licéité, leur portée et leur authenticité. Un avis juridique doit être obtenu, le cas échéant.

Seules les données à caractère personnel légalement ou raisonnablement nécessaires doivent être divulguées.

19. Gestion des violations de données à caractère personnel

Toute violation de données à caractère personnel suspectée ou confirmée doit être signalée immédiatement au moyen du processus de signalement des incidents de PECB. Le personnel ne doit pas retarder le signalement en tentant de mener une enquête de manière indépendante.

PECB doit :

- Contenir l'incident et préserver les preuves pertinentes ;
- Identifier les systèmes, registres, catégories de données, volumes approximatifs et personnes concernés ;
- Évaluer la cause, l'impact, la vraisemblance et la gravité du préjudice ;
- Déterminer les exigences et délais de notification applicables ;
- Notifier les autorités compétentes et les personnes concernées lorsque cela est requis ;
- Documenter l'évaluation, les décisions et les notifications ;
- Mettre en œuvre des actions correctives et préventives ; et
- Examiner l'efficacité de la réponse.

Toutes les violations doivent être enregistrées, y compris celles qui ne nécessitent pas de notification externe.

Lorsque la PDPA de Singapour s'applique, PECB doit évaluer si une notification à la Personal Data Protection Commission et aux personnes concernées est requise dans les délais prescrits.

Lorsque le RGPD s'applique, PECB doit évaluer si une notification à l'autorité de contrôle compétente et une communication aux personnes concernées sont requises.

Les sous-traitants, les intermédiaires de données, les prestataires de services et les partenaires doivent être tenus contractuellement de notifier à PECB les violations pertinentes sans retard injustifié.

Les employés et les sous-traitants ne doivent pas notifier de manière indépendante les personnes concernées, les autorités, les clients, les partenaires ou les médias, sauf autorisation. Le délégué à la protection des données doit être chargé de gérer la violation concernée et de communiquer à ce sujet avec les parties prenantes pertinentes.

19.1. Formation, surveillance et conformité

Le personnel ayant accès à des données à caractère personnel doit recevoir une formation appropriée en matière de protection de la vie privée et de sécurité de l'information :

- Dès son arrivée chez PECB ;
- Périodiquement par la suite ;
- Lorsque ses responsabilités changent de manière substantielle ; et
- À la suite de changements importants d'ordre juridique, politique, systémique ou liés aux risques.

Une formation spécifique au rôle doit être dispensée, le cas échéant, au personnel participant au traitement des demandes des personnes concernées, au marketing, aux ressources humaines, aux technologies de l'information, à la sécurité de l'information, aux examens, à la certification, à la gestion des partenaires, à la réponse aux incidents ou aux traitements à haut risque.

PECB doit évaluer la conformité au moyen de mesures proportionnées :

- Revues de la protection de la vie privée et des risques ;
- Audits internes ;
- Tests de sécurité ;
- Surveillance des actions correctives.

Les non-conformités, faiblesses et violations doivent être documentées et traitées. Les problèmes importants doivent être signalés au délégué à la protection des données et à la direction.

Le non-respect peut entraîner des mesures disciplinaires, une restriction des accès, des recours contractuels, la cessation de l'emploi ou de la collaboration, une action en justice ou un signalement aux autorités de réglementation lorsque cela est requis.

20. Exceptions à la Politique

Une exception à la présente Politique ne peut être approuvée que lorsque :

- Un besoin professionnel, légal, réglementaire ou technique documenté existe ;
- Les risques liés à la protection de la vie privée et à la sécurité ont été appréciés ;
- Des garanties alternatives appropriées sont mises en œuvre ;
- Le délégué à la protection des données approuve l'exception ;
- L'exception est limitée quant à sa portée et à sa durée ; et
- L'exception fait l'objet d'une revue périodique.

Aucune exception ne peut autoriser un traitement illicite.

21. Revue de la Politique

La présente Politique doit être revue au moins une fois par an et lorsqu'il existe :

- Un changement important de la législation applicable ;
- Un changement important dans la structure, les sites d'exploitation, les systèmes, les services ou les activités de traitement de PECB ;
- Une violation importante de données à caractère personnel ;
- Une constatation réglementaire, d'accréditation ou d'audit ;
- Un changement important des risques liés à la protection de la vie privée ou des responsabilités organisationnelles.

Le délégué à la protection des données doit coordonner la revue.

22. Contact et signalement

Les questions, préoccupations, demandes des personnes concernées, violations suspectées de données à caractère personnel ou violations potentielles de la Politique doivent être signalées au :

Délégué à la protection des données
E-mail : dpo@pecb.com

Spécialiste des opérations de sécurité de l'information
E-mail: information.security@pecb.com

Centre d'aide du service clientèle de PECB
E-mail: support@pecb.com

Les personnes concernées de l'EEE peuvent également contacter le représentant dans l'EEE établi à Lisbonne, au Portugal.

Représentant dans l'EEE
E-mail: gdpr.representative@pecb.com