PECB BEYOND RECOGNITION

Manuel du candidat

Certifié(e) conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL

Table des matières

SECTION I : INTRODUCTION

À propos de PECB

PECB est un organisme de certification qui propose des services d'éducation[1] et de certification de personnes selon la norme ISO/IEC 17024, dans un large éventail de disciplines.

Nous aidons les professionnels à faire preuve d'engagement et de compétence en leur fournissant des services d'évaluation et de certification en fonction de normes reconnues internationalement. Notre mission est de fournir des services qui inspirent la confiance, l'amélioration continue, assurent la reconnaissance et profitent à la société dans son ensemble.

Les principaux objectifs de PECB sont les suivants :

1. Établir les exigences minimales nécessaires à la certification des professionnels
2. Examiner et vérifier les qualifications des candidats pour s'assurer qu'ils sont éligibles à la certification
3. Développer et maintenir des évaluations de certification fiables
4. Délivrer des certifications aux candidats qualifiés, tenir des registres et publier un répertoire des détenteurs de certifications valides
5. Établir les exigences pour le renouvellement périodique de la certification et veiller au respect de ces exigences
6. S'assurer que les candidats respectent les normes éthiques dans leur pratique professionnelle
7. Représenter ses membres, le cas échéant, dans les questions d'intérêt commun
8. Promouvoir les avantages de la certification auprès des organisations, des employeurs, des fonctionnaires, des praticiens dans des domaines connexes et auprès du public

[1] Éducation fait référence aux formations développées par PECB, et offertes dans le monde entier par les Revendeurs PECB.

Valeur de la certification PECB

Reconnaissance mondiale

Les certifications PECB sont internationalement reconnues et approuvées par de nombreux organismes d'accréditation, de sorte que les professionnels qui les obtiennent bénéficient de notre reconnaissance sur les marchés nationaux et internationaux.

La valeur des certifications de PECB est validée par l'accréditation de l'International Accreditation Service (IAS-PCB-111), du United Kingdom Accreditation Service (UKAS-No. 21923) et du Korean Accreditation Board (KAB-PC-08) selon la norme ISO/IEC 17024 - Exigences générales relatives aux organismes procédant à la certification de personnes. La valeur des programmes de certification de PECB est validée par l'accréditation de l'ANSI National Accreditation Board (ANAB-Accreditation ID 1003) selon ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB est membre associé de l'Independent Association of Accredited Registrars (IAAR), membre à part entière de l'International Personnel Certification Association (IPC), membre signataire de l'IPC MLA, et membre du Club EBIOS, du CPD Certification Service, du CLUSIF, de Credential Engine et de l'ITCC. En outre, PECB est un partenaire de publication approuvé (APP) par le Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) pour la norme Cybersecurity Maturity Model Certification (CMMC), est approuvé par le Club EBIOS pour offrir la certification EBIOS Risk Manager Skills, et est approuvé par la CNIL (Commission Nationale de l'Informatique et des Libertés) pour offrir la certification DPO. Pour plus d'informations, cliquez ici.

Des produits et des services de haute qualité

Nous sommes fiers de fournir à nos clients des produits et des services de haute qualité qui répondent à leurs besoins et à leurs exigences. Tous nos produits sont soigneusement préparés par une équipe d'experts et de professionnels sur la base des meilleures pratiques et méthodologies.

Conformité aux normes

Nos certifications et nos programmes de certification démontrent la conformité aux normes ISO/IEC 17024 et ASTM E2659. Ils garantissent que les exigences de la norme ont été respectées et validées avec la cohérence, le professionnalisme et l'impartialité qui s'imposent.

Un service orienté vers le client

Nous sommes une entreprise orientée vers le client et nous traitons tous nos clients avec valeur, importance, professionnalisme et honnêteté. PECB dispose d'une équipe d'experts chargés de répondre aux demandes, aux questions et aux besoins. Nous faisons de notre mieux pour maintenir un délai de réponse maximum de 24 heures sans compromettre la qualité des services.

Flexibilité et commodité

Les possibilités d'apprentissage en ligne rendent votre parcours professionnel plus pratique, car vous pouvez programmer vos sessions d'apprentissage en fonction de votre mode de vie. Cette flexibilité vous donne plus de temps libre, vous offre davantage de possibilités d'avancement professionnel et réduit les coûts.

Code de déontologie de PECB

Les professionnels de PECB sont tenus de :

1. D'adopter un comportement professionnel lors de la prestation des services en faisant preuve d'honnêteté, de précision, d'équité et d'indépendance
2. Agir à tout moment dans les services qu'ils assurent, uniquement dans le meilleur intérêt de leur employeur, de leurs clients, du public et de la profession, conformément au présent Code de déontologie et à d'autres normes professionnelles
3. Faire montre de compétence et la développer dans leurs domaines respectifs et s'efforcer d'améliorer continuellement leurs compétences et leurs connaissances
4. N'offrir que des services pour lesquels ils sont qualifiés et compétents et informer adéquatement les clients de la nature des services proposés, y compris de toute préoccupation ou de tout risque pertinent
5. Informer leur employeur ou leur client de tout intérêt commercial ou de toute affiliation qui pourrait influencer ou altérer leur jugement
6. Préserver la confidentialité des informations de tout employeur ou client actuel ou ancien pendant la prestation des services
7. Se conformer à toutes les lois et réglementations applicables dans les juridictions du pays où les prestations de services ont été effectuées
8. Respecter la propriété intellectuelle et les contributions d'autrui
9. Ne pas communiquer intentionnellement des informations fausses ou falsifiées susceptibles de compromettre l'intégrité du processus d'évaluation d'un candidat à une certification PECB ou à un programme de certification PECB
10. Ne pas se faire passer à tort ou de manière frauduleuse pour des représentants de PECB
11. Ne pas utiliser abusivement le logo, les certifications ou les certificats de PECB
12. Ne pas agir d'une manière qui pourrait nuire à la réputation de PECB, à ses certifications ou à ses programmes de certification
13. Coopérer pleinement à l'enquête menée à la suite d'une infraction présumée au Code de déontologie

NOTE : Pour des exemples spécifiques de violation et de conséquences, veuillez vous référer à la Politique applicable en cas de violation du Code de déontologie de PECB | PECB.

Introduction à la certification « Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL**»**

Le nombre d'organisations exerçant des activités transfrontalières étant en constante augmentation, la protection des données à caractère personnel ainsi que les lois et droits en la matière deviennent de plus en plus cruciaux pour les organisations et les individus. Des garanties et des mesures appropriées doivent être mises en œuvre pour assurer la sécurité de ces données, droit fondamental des personnes physiques. Cette nécessité de sécuriser les données, de prévenir les violations des données à caractère personnel et de garantir un traitement sûr des données est plus grande que jamais et augmentera régulièrement.

Afin de protéger et de respecter les libertés et droits fondamentaux des personnes physiques à l'égard du traitement de leurs données à caractère personnel, le Parlement européen a approuvé la proposition de la Commission européenne pour la publication du Règlement général sur la protection des données, qui est entré en vigueur après sa publication.

Champs d'application matériel et territorial

1. *Le RGPD s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.*
2. *Le RGPD s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.*
3. *Le RGPD s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:*
   a) *à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou*
   b) *au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.*

Étant donné que la protection des données à caractère personnel, la prévention d'une violation de ces données et la sécurité du traitement sont essentielles pour toutes les organisations opérant au sein ou en coopération avec des organisations établies dans l'UE, le besoin de délégués à la protection des données certifiés augmente sans cesse. Les employeurs d'aujourd'hui ne se contentent pas de rechercher des professionnels de la protection des données ; ils veulent la preuve que ces professionnels possèdent un ensemble prédéterminé de connaissances et de compétences. Les organisations accordent désormais une grande importance à l'embauche d'experts de la sécurité accrédités et préparés à relever les défis d'aujourd'hui et de demain en matière de sécurité et d'incidents liés aux données à caractère personnel.

Il est important de préciser que les certifications de PECB ne sont pas une licence ou une simple adhésion. Il s'agit d'une reconnaissance par les pairs qu'une personne a démontré sa maîtrise et sa compréhension d'un ensemble de compétences. Les certifications PECB sont accordées aux candidats qui peuvent fournir la preuve de leur expérience et qui ont réussi un examen normalisé dans le domaine de la certification.

Le présent document présente la certification « Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL Il contient également des informations sur le processus par lequel les candidats peuvent obtenir et renouveler leur certification. Il est très important que vous lisiez toutes les informations contenues dans ce manuel **avant** de remplir et de soumettre votre candidature. Si vous avez des questions après avoir lu le Manuel du candidat, veuillez contacter directement le Service de la certification de PECB à l'adresse suivante : certification.team@pecb.com.

SECTION II : PROCESSUS DE CERTIFICATION ET PRÉPARATION, POLITIQUES ET RÈGLEMENTS RELATIFS À L'EXAMEN DE PECB

Prérequis spécifiques à la certification Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL

L'expérience professionnelle minimale requise est :

- Au moins deux ans d'expérience professionnelle dans des projets, activités ou tâches liés aux missions du délégué à la protection des données à caractère personnel ; ou
- Justifier d'une expérience professionnelle d'au moins 2 ans ainsi que d'une formation d'au moins 35 heures en matière de la protection des données personnelles reçues par un organisme de formation

Cette information est présentée par le candidat dans la demande d'admissibilité.

Évaluation des demandes d'admissibilité

Le Service de certification évaluera chaque demande afin de valider l'admissibilité du candidat à la certification. Le candidat dont la demande est examinée en sera informé par écrit et disposera d'un délai raisonnable pour fournir tout document supplémentaire si nécessaire. Si le candidat ne répond pas dans le délai imparti ou ne fournit pas les documents requis dans le délai imparti, ou ne remplit pas les prérequis d'expérience professionnelle ou de formation, la demande sera refusée.

Si le candidat remplit les prérequis, la demande d'admissibilité est approuvée et le candidat peut continuer à la préparation et programmation de l'examen.

Préparer et programmer l'examen

Les candidats sont responsables de leur propre étude et de leur préparation aux examens de certification. Aucun ensemble spécifique de cours ou de programmes d'études n'est requis dans le cadre du processus de certification. Toutefois, la participation à une session de formation peut augmenter de manière significative les chances de réussite à l'examen PECB.

Pour programmer un examen de certification PECB, les candidats doivent contacter l'un de nos revendeurs qui proposent des sessions de formation et d'examen. Les candidats trouveront un Revendeur de formations dans une région donnée sur la page Liste des revendeurs. Le calendrier des sessions de formation PECB est également disponible sous l'onglet Calendrier des formations.

Pour en savoir plus sur les examens, les domaines de compétences et les énoncés de connaissances, veuillez vous référer à la section III du présent document.

Frais de demande d'examen et de certification

PECB propose aussi les examens directement, où un candidat peut se présenter à l'examen sans assister à la formation. Les prix sont les suivants :

- Examen : 1000 $ US
- Frais de demande de certification : 500 $ US

Pour tous les candidats qui ont suivi la formation et passé l'examen auprès d'un revendeur PECB, le coût de la session de formation comprend les frais associés à l'examen (examen et première reprise) et à la demande de certification.

Domaines de compétence

L'examen «Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL» a pour objectif de veiller à ce que le candidat possède l'expertise nécessaire pour aider une organisation à mettre en œuvre, à gérer et à maintenir un cadre de conformité à la protection des données basé sur le RGPD.

Cet examen s'adresse aux :

- Responsables de projet ou consultants souhaitant préparer et soutenir une organisation dans la mise en œuvre des nouvelles procédures et l'adoption des nouvelles exigences présentées dans le RGPD
- Personnes certifiées et cadres supérieurs responsables de la protection des données à caractère personnel d'une entreprise et de la gestion des risques
- Membres d'une équipe de sécurité de l'information, de gestion des incidents et de continuité d'activité
- Conseillers spécialisés en sécurité des données à caractère personnel
- Experts techniques et experts de la conformité envisageant un poste de délégué à la protection des données

L'examen couvre les domaines suivants :

- **Domaine 1 :** Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité
- **Domaine 2 :** Responsabilité
- **Domaine 3 :** Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

PECB

Domaine 1 : Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité

Objectif principal : S'assurer que le candidat à la certification « Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL» peut comprendre et interpréter les objectifs, le champ d'application, les définitions, les concepts, les principes de protection des données et les droits des personnes concernées selon le RGPD

Compétences	Énoncés des connaissances
1. Capacité à comprendre l'importance du Comité Européen de la Protection des Données, de ses membres et de ses fonctions	1. Connaissance de l'importance du droit fondamental en matière de protection des personnes physiques en relation avec le traitement des données à caractère personnel
2. Capacité à expliquer le champ d'application matériel et territorial du RGPD, et où il s'applique	2. Connaissance des différents facteurs, tels que l'intégration économique et sociale, qui affectent la coopération entre les États membres en matière d'échange de données à caractère personnel
3. Capacité à comprendre les définitions et les concepts importants de la protection des données nécessaires pour se conformer à la réglementation	3. Connaissance des implications commerciales du RGPD
4. Capacité à expliquer les principaux problèmes et défis liés à la conformité au RGPD	4. Connaissance des principales définitions du RGPD qui fournissent des informations précieuses pour une compréhension et une mise en œuvre efficaces d'un cadre de conformité basé sur le RGPD
5. Capacité à comprendre les principes de protection des données requis par le RGPD	5. Connaissance des principes clés en matière de protection des données qui fournissent des informations précieuses pour une compréhension et une mise en œuvre efficaces d'un cadre de conformité basé sur le RGPD
6. Capacité à mettre en œuvre les mesures nécessaires pour assurer le respect des principes de base du traitement des données à caractère personnel, notamment la responsabilité, la transparence, la licéité, la limitation des finalités, la minimisation des données, la limitation du stockage	6. Connaissance des mesures appropriées pour assurer le respect des principes de base du traitement des données à caractère personnel
7. Capacité à identifier les bases légales pour le traitement des données	7. Connaissances sur les concepts clés fournis par le RGPD, y compris les responsables de traitement, les sous-traitants, le DPO, la restriction du traitement, les données à caractère personnel, les données génétiques, etc.
8. Capacité à comprendre les concepts clés du RGPD	8. Connaissance des droits des personnes concernées et de l'accès aux données à caractère personnel
9. Capacité à comprendre les droits de la personne concernée	9. Connaissance des conditions de licéité du traitement
10. Capacité à comprendre quelles sont les mesures nécessaires pour assurer la conformité et protéger le droit des personnes concernées	10. Connaissance des informations requises fournies à la personne concernée lors de la collecte des données auprès de celle-ci
11. Capacité à établir des procédures destinées à recevoir et à gérer les demandes d'exercice des droits et libertés de la personne concernée	11. Connaissance de l'obligation de fournir des informations à la personne concernée sous une forme concise, transparente, intelligible et facilement accessible, ainsi que des outils, méthodes et mécanismes à utiliser
12. Capacité à comprendre les exigences relatives aux informations à fournir à la personne concernée pour l'exercice de ses droits	12. Connaissances sur la manière de mener une analyse des écarts et de déterminer ce qu'une organisation veut réaliser en mettant en œuvre le RGPD
13. Capacité à déterminer et à établir des mesures appropriées afin de fournir des informations transparentes à la personne concernée	13. Connaissance de l'importance du business case et de son contenu
14. Capacité à préparer la mise en œuvre du RGPD	
15. Capacité à élaborer et à présenter un business case	
16. Capacité à effectuer une analyse des écarts	
17. Capacité à établir l'équipe de projet de conformité au RGPD	
18. Capacité à déterminer les ressources nécessaires pour la mise en œuvre du projet de conformité au RGPD	

19. Capacité à rédiger et à passer en revue un plan de projet 20. Capacité à comprendre la désignation du délégué à la protection des données 21. Capacité à comprendre les tâches et responsabilités du délégué à la protection des données 22. Capacité à comprendre les principales activités du DPO 23. Capacité à créer des modèles de politique 24. Capacité à rédiger une politique de protection des données 25. Capacité à publier une politique de protection des données 26. Capacité à identifier l'existence de transferts de données en dehors de l'UE/EEE vers des pays tiers ou des organisations internationales 27. Capacité à mener des audits internes 28. Capacité à désigner une personne responsable pour mener l'audit interne 29. Capacité à effectuer des activités d'audit 30. Capacité à établir et à réviser une liste de contrôle d'audit du RGPD	14. Connaissance des rôles et responsabilités du sponsor du projet, du gestionnaire de projet, de l'équipe de gestion de projet et des parties intéressées 15. Connaissance des types de ressources nécessaires pour mettre en œuvre efficacement le projet de conformité au RGPD 16. Connaissance de l'importance du plan de projet et des raisons d'utiliser le plan de projet 17. Connaissance des principaux éléments du plan de projet, y compris la charte du projet, la structure de la répartition des travaux, le coût estimatif, les livrables du projet, etc. 18. Connaissances sur la façon d'examiner les objectifs et les facteurs de réussite du projet, la méthode proposée, les produits livrables, les rôles et responsabilités et les documents de projet 19. Connaissance des principaux avantages de l'engagement de la direction et des avantages attendus de la mise en œuvre du projet de conformité au RGPD 20. Connaissance du processus requis pour désigner un délégué à la protection des données 21. Connaissance des qualités professionnelles du délégué à la protection des données désigné 22. Connaissance des exigences du RGPD concernant les tâches du DPO 23. Connaissance des impacts qui influencent les performances du DPO, y compris le soutien au responsable du traitement et au sous-traitant 24. Connaissance des qualifications professionnelles requises pour la nomination d'un DPO 25. Connaissances sur la façon d'allouer les ressources nécessaires 26. Connaissances sur la manière de mettre en place de nouvelles politiques de données, de réduire l'impact des risques connus, d'encourager l'éducation et la formation, de définir des règles de consentement des clients et de créer une politique de données pour les données obsolètes 27. Connaissance du processus général d'élaboration d'une politique 28. Connaissance des objectifs de la politique de protection des données 29. Connaissance de la publication de la politique de protection des données 30. Connaissances sur la manière de communiquer la politique de protection des données approuvée et d'évaluer si ses objectifs sont atteints 31. Connaissance des instruments juridiques fournis par le RGPD pour les transferts de données en dehors de l'UE/EEE vers des pays tiers ou des organisations internationales (codes de conduite approuvés, mécanismes de certification approuvés, transferts fondés sur des décisions adéquates, règles d'entreprise

	contraignantes, clauses contractuelles standard et dérogations) 32. Connaissance du rôle de l'auditeur interne en ce qui a trait au RGPD 33. Connaissance des rôles et responsabilités de la personne désignée pour effectuer un audit interne 34. Connaissance des activités d'audit, y compris la collecte d'informations provenant de différentes sources d'information, l'utilisation de procédures d'audit appropriées, la collecte d'éléments probants d'audit, l'évaluation des éléments probants par rapport aux critères d'audit, le rapport d'audit et la conclusion d'audit 35. Connaissance des éléments de la liste de contrôle du RGPD, y compris la gouvernance et la responsabilité des données, les politiques de confidentialité, les notifications de violation, les traitements de données et les transferts internationaux, la légalité du traitement et du consentement, les droits des personnes concernées

Domaine 2 : Responsabilité

Objectif principal : S'assurer que le candidat à la certification « Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL» peut comprendre et déterminer les principales missions et responsabilités du responsable du traitement, du sous-traitant et du délégué à la protection des données, l'importance des activités de traitement, et s'assurer qu'il comprend le processus de cartographie des données et l'analyse d'impact relative à la protection des données (AIPD)

Compétences	Énoncés des connaissances
1. Capacité à comprendre l'importance du responsable du traitement et du sous-traitant 2. Capacité à déterminer les rôles et responsabilités du responsable du traitement et du sous-traitant 3. Capacité à comprendre le traitement sous l'autorité du responsable du traitement et du sous-traitant 4. Capacité à comprendre le rôle du DPO en relation avec l'analyse d'impact relative à la protection des données (AIPD) et les activités de traitement 5. Capacité à comprendre le processus de cartographie des données 6. Capacité à comprendre l'importance du processus de cartographie des données 7. Capacité à comprendre les pratiques recommandées de cartographie des données 8. Capacité à comprendre la cartographie des flux de données et le diagramme de flux de données 9. Capacité à comprendre l'importance du registre des activités de traitement 10. Capacité à déterminer à quel moment l'organisation est tenue de tenir un registre des activités de traitement dont elle est responsable 11. Capacité à rédiger et à tenir à jour les registres prévus à l'article 30 du RGPD 12. Capacité à élaborer et à tenir à jour les registres des activités de traitement 13. Capacité à comprendre ce qui est couvert par l'analyse d'impact relative à la protection des données (AIPD) 14. Capacité à comprendre le processus itératif pour réaliser une analyse d'impact relative à la protection des données (AIPD) 15. Capacité à déterminer quand une analyse d'impact relative à la protection des données (AIPD) est nécessaire 16. Capacité à effectuer une AIPD et à fournir des conseils à ce sujet 17. Capacité à évaluer les risques de sécurité 18. Capacité à identifier les violations de protection des données à caractère personnel qui	1. Connaissance des exigences du RGPD qui fournissent des informations concernant le responsable du traitement et le sous-traitant 2. Connaissance des mesures techniques et organisationnelles appropriées qui doivent être mises en œuvre par le responsable du traitement et le sous-traitant 3. Connaissance de qui doit et ne doit pas traiter les données à caractère personnel selon les exigences requises par le RGPD 4. Connaissance de l'importance du traitement des données à caractère personnel 5. Connaissance en matière d'élaboration de cartographies de données entre différents modèles de données et détermination des types de données à caractère personnel traitées par une organisation 6. Connaissances sur la manière d'élaborer et de tenir à jour les enregistrements des activités de traitement 7. Connaissance des étapes du processus de cartographie de données 8. Connaissances sur les catégories de données stockées, qui les possède et a accès aux données stockées et à quels destinataires les données sont divulguées 9. Connaissance des pratiques recommandées de cartographie des données telles que la construction et la maintenance 10. Connaissance des éléments clés des cartographies des flux de données et création d'un diagramme de flux de données 11. Connaissance de l'importance de l'AIPD et des traitements qu'elle traite 12. Connaissance des étapes du processus itératif pour la réalisation d'une AIPD, y compris les étapes telles que le traitement prévu, l'évaluation de la nécessité, les mesures prévues pour démontrer la conformité, l'évaluation des risques, les mesures prévues pour traiter le risque, la documentation, la surveillance et la revue 13. Connaissance des critères à prendre en compte lorsque le traitement de données à caractère personnel pourrait entraîner un risque élevé

nécessitent une notification à l'autorité de contrôle compétente 19. Capacité à comprendre l'importance de notifier toute violation de données à caractère personnel sans retard injustifié 20. Capacité à identifier les violations de données à caractère personnel qui doivent être communiquées à la personne concernée 21. Capacité à communiquer la violation de données à caractère personnel à la personne concernée 22. Capacité à identifier les mesures de protection des données dès la conception et à intégrer les garanties nécessaires dans le traitement 23. Capacité à mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel nécessaires aux activités de traitement sont collectées	14. Connaissance des mesures à mettre en œuvre si l'analyse d'impact relative à la protection des données indique que le traitement entraînera un risque élevé 15. Connaissance des avantages de l'AIPD, y compris l'identification des impacts sur la vie privée, l'examen d'un nouveau système d'information, la contribution à la conception de la protection de la vie privée, le partage et l'atténuation des risques pour la vie privée avec les parties prenantes, etc. 16. Connaissance des directives WP29 et ISO/IEC 29134 sur la conduite d'une analyse d'impact relative à la protection des données 17. Connaissance des principaux défis auxquels les organisations peuvent être confrontées lors de la mise en œuvre du RGPD, y compris la conformité aux principes de base, des droits des personnes concernées, la notification des violations de données et les problèmes pouvant apparaître 18. Connaissance du temps nécessaire pour informer les autorités de contrôle de la violation des données à caractère personnel 19. Connaissance des méthodes de communication appropriées en tant que moyen d'informer la personne concernée en cas de violation de données à caractère personnel 20. Connaissances sur la sensibilisation à l'importance de la protection des données à caractère personnel, la documentation des informations, la reconnaissance des droits relatifs aux personnes concernées, les violations de données, les données relatives aux enfants et autres exigences du RGPD 21. Connaissance du processus d'évaluation des risques et de la hiérarchisation des risques 22. Connaissance des mesures techniques et organisationnelles pour assurer la protection des données dès la conception telles que le chiffrement des données, l'anonymisation et la pseudonymisation

Domaine 3 : Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

Objectif principal : S'assurer que le candidat à la certification « Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL» peut déterminer les mesures nécessaires pour garantir le traitement sécurisé des données à caractère personnel et la conformité au RGPD, interpréter la relation entre le RGPD, la sécurité de l'information, la continuité d'activité et la gestion des incidents, et évaluer, surveiller et mesurer les performances du projet de conformité au RGPD

Compétences	Énoncés des connaissances
1. Capacité à définir une structure organisationnelle pour la gestion de la protection des données	1. Connaissances sur la manière de développer une structure de gouvernance pour la protection des données qui répond pleinement aux exigences telles que le soutien important de la direction
2. Capacité à comprendre la relation entre le RGPD et la sécurité de l'information	2. Connaissances sur les aspects de la sécurité de l'information qui peuvent être compatibles avec le RGPD
3. Capacité à déterminer les mesures techniques et organisationnelles nécessaires pour assurer la sécurité du traitement	3. Connaissance des avantages de la stratégie de cybersécurité centrée sur les données, y compris l'amélioration de la sensibilisation à la sécurité des données au sein d'une organisation, l'identification des données les plus cruciales, la réduction des coûts, l'augmentation de l'efficacité des solutions DLP, la cohérence des politiques de sécurité
4. Capacité à assurer la sécurité des données à caractère personnel, y compris leur traitement	4. Connaissances sur les 10 étapes de la cybersécurité, à savoir le régime de gestion des risques informationnels, la configuration de la sécurité, la sécurité du réseau, la gestion des droits d'utilisateurs, la formation des utilisateurs, la gestion des incidents, la protection contre les logiciels malveillants, la surveillance, le contrôle des supports amovibles, le travail à domicile et mobile
5. Capacité à comprendre la relation entre le RGPD et la continuité d'activité	5. Connaissance des étapes des stratégies de sécurité de l'information et des principaux aspects liés à la sécurité tels que les personnes, les processus et la technologie
6. Capacité à définir les étapes qui aident les organisations à assurer la conformité avec le RGPD	6. Connaissance des mesures techniques et organisationnelles telles que la minimisation des données, le chiffrement des données, la pseudonymisation et la sécurité physique
7. Capacité à gérer et à maintenir la relation avec l'autorité de surveillance, y compris, entre autres, la communication, la consultation, la réponse à leurs demandes et la prise en compte de leurs demandes	7. Connaissances sur la manière d'assurer la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement
8. Capacité à comprendre la relation entre le RGPD et la gestion des incidents	8. Connaissances sur la manière de restaurer en temps opportun la disponibilité et l'accès aux données à caractère personnel en cas d'incident physique ou technique
9. Capacité à préparer un plan d'intervention en cas d'incident	9. Connaissances sur les parties de la continuité d'activité qui peuvent être compatibles avec le RGPD
10. Capacité à élaborer, à mettre en œuvre et à diriger des programmes de formation et de sensibilisation en matière de protection des données à l'intention du personnel et de la direction	10. Connaissances sur les aspects de la gestion des incidents pouvant être compatibles avec le RGPD
11. Capacité à comprendre et à déterminer des objectifs de mesure	
12. Capacité à déterminer quelles activités, processus et systèmes devraient être surveillés	
13. Capacité à rapporter les résultats de mesure de la performance du projet de conformité au RGPD	
14. Capacité à mener des évaluations du projet de conformité au RGPD pour assurer une stabilité, une adéquation et une efficacité constantes	
15. Capacité à comprendre les principes et les concepts liés à l'amélioration continue	
16. Capacité à améliorer continuellement le projet de conformité au RGPD	

	11. Connaissances sur la façon d'établir un plan d'intervention en cas d'incident en fonction du processus de gestion des incidents 12. Connaissances sur les contrôles à mesurer et à surveiller 13. Connaissances sur quand surveiller, mesurer, analyser et évaluer les performances du projet de conformité au RGPD 14. Connaissances sur qui surveillera, mesurera, analysera et évaluera la performance du projet de conformité au RGPD 15. Connaissances sur la façon de surveiller les activités, les processus et les systèmes, y compris la gestion des incidents, la gestion de la sécurité physique et environnementale, le processus d'évaluation des risques, la sensibilisation à la sécurité et la formation, etc. 16. Connaissances sur l'établissement des rapports des résultats de mesure en utilisant des fiches de résultats ou des tableaux de bord stratégiques, des tableaux de bord tactiques et opérationnels, des rapports et des jauges 17. Connaissance des principaux concepts liés à l'amélioration continue 18. Connaissances sur la façon de surveiller en permanence les facteurs de changement qui influent sur l'efficacité des projets de conformité au RGPD

Sur la base de ces trois domaines et de leur pertinence, l'examen comprend cent (100) questions. L'examen à choix multiple évalue les compétences et le savoir-faire (résumés dans les énoncés de connaissances) selon les critères suivants :

Domaine 1 : Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité : 50 % des questions
Domaine 2 : Responsabilité : 30 % des questions
Domaine 3 : Mesures techniques et organisationnelles pour la sécurité des données au regard des risques : 20 % des questions

Pour chacun des domaines, au moins 30 % des questions sont présentées sous forme de cas pratiques, comme le résume le tableau suivant :

		Points par question	Nombre de questions par domaine de compétence	Nombre de questions présentées sous forme de cas pratiques	Nombre de points par domaine de compétence	% de points par domaine de compétence
Domaines de compétence	Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité	1	50	17 (34 %)	50	50 %
	Responsabilité		30	15 (50 %)	30	30 %
	Mesures techniques et organisationnelles pour la sécurité des données au regard des risques		20	6 (30 %)	20	20 %
	Total des points		100			

La note de passage est établie à 75 %. De plus, pour chaque domaine, au moins 50 % des réponses doivent être réussies.

Après avoir réussi l'examen, les candidats pourront demander la certification « Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL».

Faire l’examen

Informations générales sur l’examen

Les candidats sont tenus d'être présents au moins 30 minutes avant le début de l'examen. Les candidats qui arrivent en retard ne disposeront pas de temps supplémentaire pour compenser leur retard et pourraient se voir refuser l'accès à l'examen.

Les candidats doivent être en possession d'une carte d'identité valide (carte d'identité nationale, permis de conduire ou passeport) et la présenter au surveillant.

L’examen dure trois heures (3 h).

Si la demande en est faite le jour de l'examen, un délai supplémentaire de 30 minutes peut être accordé aux candidats qui passent l'examen dans une langue autre que leur langue maternelle.

Format et type d’examen PECB

Examen au format papier : L’examen est imprimé et les candidats ne sont autorisés à utiliser que l'examen et un stylo. L'utilisation d'appareils électroniques, tels qu’ordinateurs portables, tablettes ou téléphones, n'est pas autorisée. La session d'examen est supervisée par un surveillant agréé par PECB là où le revendeur a organisé la session de formation.

Examen à choix multiple, à livre fermé : Ce type d’examen a été choisi, car il s'est avéré efficace et efficient pour mesurer et évaluer les résultats d'apprentissage selon les domaines de compétence. L'examen à choix multiple peut être utilisé pour évaluer la compréhension d'un candidat sur de nombreux sujets, y compris des concepts simples ou complexes. Pour répondre à ces questions, les candidats devront appliquer les différents principes de la formation, analyser des problèmes, évaluer des alternatives, combiner plusieurs concepts ou idées, etc.
Les questions à choix multiple sont basées sur un scénario, ce qui signifie qu'elles sont élaborées sur la base d'un scénario que les candidats sont invités à lire et qu'ils doivent fournir des réponses à une ou plusieurs questions liées à ce scénario.

Dans la mesure où un apprentissage et une mémorisation plus approfondis sont encouragés, cet examen se fera à livre fermé. Vous trouverez ci-dessous un échantillon de questions d'examen.
Pour chaque question, quatre réponses possibles sont données, dont une seule est correcte.

Toute tentative de copie, de collusion ou de tricherie pendant l’examen entraînera automatiquement un échec.

Exemples de questions d’examen

Question 1 :
L'entreprise A a reçu une amende de 50 000 € après le vol d'une clé USB contenant les données à caractère personnel de plus de 1 000 personnes. Après une enquête interne, l'entreprise a constaté qu'il s'agissait d'une pratique courante parmi ses employés : les employés transféraient des données à caractère personnel de leurs dossiers personnels vers des clés USB afin d'accéder aux données de l'extérieur des bureaux au besoin. Lorsqu'on leur a posé la question, les employés ont déclaré qu'ils avaient parfois besoin d'avoir accès à des données à l'extérieur de leurs bureaux.

Laquelle des mesures suivantes serait particulièrement efficace pour protéger les données contre l'accès non autorisé tout en n'empêchant pas les employés de faire leur travail ?

A. Établissement des sauvegardes

B. Réalisation d'une analyse d'impact relative à la protection des données
C. **Chiffrement**
D. Interdire l'utilisation des données à caractère personnel en dehors des bureaux

Question 2 :
Lequel des énoncés suivants est correct ?

A. Le RGPD recommande la mise en œuvre de mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque
B. **Le RGPD exige la mise en œuvre de mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au risque**
C. ISO/IEC 27001 recommande la mise en œuvre d'un système de management de la sécurité de l'information
D. Le RGPD recommande la mise en œuvre de mesures techniques appropriées pour éviter le risque

Transmission des résultats d'examen

Les résultats d'examens seront communiqués par e-mail dans un délai de 2 à 4 semaines suivant la date de l'examen. Les seuls résultats possibles sont la réussite ou l'échec ; aucune note ne sera incluse.

Les candidats qui réussissent l'examen et remplissent toutes les exigences de certification pourront obtenir la certification «Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL».

En cas d'échec à l'examen, une liste des domaines dans lesquels le candidat a obtenu une note inférieure à la note de passage sera ajoutée à l'e-mail pour aider les candidats à mieux se préparer à une reprise.

Politique de reprise d'examen

Un candidat peut reprendre un examen autant de fois qu'il le souhaite. Il existe néanmoins certains délais à respecter entre les reprises d'examen.

- Si le candidat échoue à l'examen à la 1re tentative, il doit attendre 15 jours à compter de la date de l'examen initial avant la prochaine tentative (1re reprise).
  Remarque : Les candidats qui ont suivi la formation chez l'un de nos partenaires et qui ont échoué à la première tentative d'examen peuvent le reprendre gratuitement dans les 12 mois à compter de la date de réception du code promotionnel, car le prix payé pour la formation comprend une première tentative d'examen et une reprise.) Autrement, des frais s'appliquent.

Pour les candidats qui échouent la reprise, PECB recommande de suivre une formation afin d'être mieux préparé à l'examen.

Pour organiser une reprise d'examen, en fonction du format de l'examen, les candidats qui ont suivi une formation doivent suivre les étapes ci-dessous :

1. Examen en ligne : lors de l'organisation de la reprise de l'examen, utilisez le code initial pour annuler les frais
2. Examen sur papier : les candidats doivent contacter le partenaire/distributeur PECB qui a organisé la session initiale pour convenir des modalités de reprise de l'examen (date, heure, lieu, coûts)

Les candidats qui n'ont pas suivi une formation auprès d'un partenaire, mais qui se sont présentés à l'examen en ligne directement avec PECB, ne sont pas concernés par cette politique. La procédure d'organisation de la reprise de l'examen est la même que pour l'examen initial.

Sécurité de l’examen

Une composante importante de la certification professionnelle est le maintien de la sécurité et de la confidentialité de l'examen. PECB compte sur le comportement éthique des titulaires et des candidats à la certification pour maintenir la sécurité et la confidentialité des examens PECB. Toute divulgation d'informations sur le contenu des examens PECB constitue une violation directe du Code de déontologie de PECB. PECB prendra des mesures à l'encontre de toute personne qui enfreint les politiques et règlements, y compris l'interdiction permanente d'obtenir les certifications PECB et la révocation de toute certification antérieure. PECB intentera également une action en justice contre les personnes ou les organisations qui enfreignent ses droits d'auteur, ses droits de propriété et sa propriété intellectuelle.

Reprogrammer l’examen

Pour tout changement concernant la date, l'heure, le lieu de l'examen ou d'autres détails, veuillez contacter online.exams@pecb.com.

Demander la certification

Les exigences pour obtenir la certification Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL sont :

- Avoir réussi l'examen de certification PECB (ou un équivalent accepté par PECB);

Avoir obtenu la validation de l'expérience professionnelle de ses références

- Avoir satisfait à toutes les autres exigences ;
- Avoir acquitté tous les frais de demande de certification.

Le candidat doit remplir le formulaire de demande de certification en ligne (accessible via son compte PECB), y compris les coordonnées des références qui seront contactées pour valider l'expérience professionnelle du candidat. Le candidat peut soumettre sa demande en plusieurs langues. Il peut choisir de payer en ligne ou d'être facturé. Pour de plus amples informations, veuillez contacter certification.team@pecb.com.

Le processus de demande de certification en ligne est très simple et ne prend que quelques minutes :

- Inscrivez-vous si ce n’est déjà fait. Vérifier vos e-mails pour activer le lien de confirmation.
- Connectez-vous pour demander la certification

Pour plus d'informations sur le processus de demande, suivez les instructions du manuel Faire une demande de certification.

La demande est approuvée dès que le Service de certification valide que le candidat remplit toutes les exigences de certification relatives au titre concerné. Un e-mail sera envoyé à l'adresse électronique fournie au cours du processus de demande pour communiquer l’état de la demande. Si la demande est approuvée, le candidat pourra télécharger la certification à partir de son compte PECB.

Renouveler la certification

Les certifications PECB sont valides pour une période de trois ans à compter de la date de délivrance. Avant la date d’échéance, les candidats doivent payer les frais, réussir la nouvelle épreuve écrite, présenter la preuve d’une (1) année d’expérience en protection des données acquise dans le courant des trois dernières années, dans des projets, activités ou tâches en lien avec les missions du délégué à la protection des données s’agissant de la protection des données ou de la sécurité de l’information, attestée par un tiers (employeur ou client et remplir les exigences pour le renouvellement de la certification. «)

Les frais pour le renouvellement de la certification des compétences du DPO de la CNIL sont de 500 $ US.

Fermeture d’un dossier

Si un candidat ne demande pas la certification dans les trois ans, son dossier sera fermé. Toutefois, même si la période de certification expire, le candidat a le droit de rouvrir son dossier. Cependant, PECB ne sera plus responsable de tout

changement concernant les conditions, les normes, les politiques et le Manuel du candidat qui étaient applicables avant la fermeture du dossier. Un candidat qui demande la réouverture de son dossier doit le faire par écrit et payer les frais requis.

SECTION III : EXIGENCES DE CERTIFICATION

Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL **Les exigences relatives à la certification « Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL» sont les suivantes :**

Titre de compétence	Examen	Expérience professionnelle (prérequis)	Autres exigences spécifiques à PECB
Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL	Examen « Certifié conformément au référentiel de certification des compétences du délégué à la protection des données de la CNIL»	• Justifier d'une expérience professionnelle d'au moins 2 ans dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données personnelles; ou • Justifier d'une expérience professionnelle d'au moins 2 ans ainsi que d'une formation d'au moins 35 heures en matière de protection des données personnelles reçue par un organisme de formation.	Signer le Code déontologie de PECB

Les principales compétences et connaissances requises par le marché sont la capacité de soutenir une organisation à assurer un niveau adéquat de sécurité du traitement des données à caractère personnel et à se conformer aux exigences du RGPD, incluant les principes de base de la sécurité des données à caractère personnel, les transferts de données à caractère personnel vers des pays tiers, la désignation d'un DPO, les droits de la personne concernée, le rôle des responsables du traitement et des sous-traitants ainsi que la mise en œuvre de mesures de sécurité techniques et organisationnelles.

L'expérience professionnelle d'au moins 2 ans dans des projets, activités ou tâches en lien avec les missions du DPO devrait suivre les bonnes pratiques et inclure les activités suivantes :

- Aider à l'application des exigences du RGPD
- Surveiller le programme de conformité au RGPD
- Conseiller sur l'analyse d'impact relative à la protection des données
- Surveiller un projet de mise en œuvre de la protection des données dans le cadre du traitement des données à caractère personnel, en conformité avec le RGPD

SECTION IV : POLITIQUES ET RÈGLEMENTS RELATIFS À LA CERTIFICATION

Références professionnelles

Pour chaque demande de certification, deux références professionnelles sont requises. Les références professionnelles doivent provenir de personnes ayant travaillé avec le candidat dans un environnement professionnel et pouvant ainsi attester de son expérience du projet RGPD, ainsi que de ses antécédents professionnels actuels et antérieurs. Les références professionnelles de personnes qui sont sous la supervision du candidat ou qui sont ses proches ne sont pas valables.

Expérience professionnelle

Le candidat doit fournir des informations complètes et exactes concernant son expérience professionnelle, notamment le titre de chaque poste, les dates de début et de fin, la description des postes, etc. Il est conseillé au candidat de résumer ses missions précédentes et actuelles, en fournissant suffisamment de détails pour décrire la nature des responsabilités de chaque emploi. Des informations plus détaillées peuvent être incluses dans le CV.

Refus de la demande de certification

PECB peut refuser la demande de certification si le candidat:

- Falsifie la demande d'admissibilité ou la demande de certification
- Enfreint les procédures d'examen
- Enfreint le Code de déontologie de PECB
- Échoue à l'examen
- N'obtient pas la validation de l'expérience professionnelle par ses références

Pour des informations plus détaillées, reportez-vous à la section ***Plainte et appel***.

Le paiement de la demande de certification n'est pas remboursable.

Suspension de la certification

PECB peut suspendre temporairement la certification si le candidat ne satisfait pas aux exigences de PECB. D'autres raisons peuvent justifier la suspension de la certification :

- Non-respect des exigences en matière de renouvellement de la certification
- PECB reçoit des plaintes excessives ou sérieuses de la part des parties intéressées (la suspension sera appliquée jusqu'à ce que l'enquête soit terminée).
- Les logos de PECB ou des organismes d'accréditation sont délibérément utilisés de manière abusive.
- Le candidat ne corrige pas l'usage abusif d'une marque de certification dans le délai déterminé par PECB.
- La personne certifiée a volontairement demandé une suspension.
- Toute autre condition jugée appropriée pour la suspension de la certification.

Révocation de la certification

PECB peut révoquer (c'est-à-dire retirer) la certification si le candidat ne satisfait pas aux exigences de PECB de certification ou de renouvellement de la certification. Le candidat n'est alors plus autorisé à se présenter comme un professionnel certifié par PECB. D'autres raisons de révocation de la certification peuvent être invoquées si le candidat :

- Non rétablissement de la certification suspendue dans le délai imparti
- Enfreint le Code de déontologie de PECB
- Fait une fausse déclaration et fournit de fausses informations sur la portée du certificat
- Déclare ou fourni de fausses informations dans la demande d’admissibilité ou la demande de certification
- Enfreint toute autre règle de PECB

Autres statuts

En plus d'être active, suspendue ou révoquée, une certification peut être retirée volontairement. Pour plus d'informations sur ces statuts et sur le statut de cessation permanente, ainsi que sur la manière de les appliquer, veuillez consulter la page État de la certification.

SECTION V : À PROPOS DES POLITIQUES GÉNÉRALES DE PECB

Code de déontologie de PECB

L'adhésion au Code de déontologie de PECB est un engagement volontaire. Il est important que les professionnels certifiés par PECB non seulement adhèrent aux principes de ce Code mais aussi qu'ils encouragent et soutiennent les autres à faire de même. Plus d'informations sont disponibles ici.

Autres examens et certifications

PECB accepte les certifications et les examens d'autres organismes de certification accrédités et reconnus. PECB évaluera les demandes par le biais de son processus d'équivalence pour décider si la ou les certifications ou examens respectifs peuvent être acceptés comme équivalents à la certification PECB respective (par exemple, la certification ISO/IEC 27001 Lead Auditor).

Non-discrimination et aménagements spéciaux

Toutes les candidatures seront évaluées objectivement, sans considération d'âge, de sexe, de race, de religion, de nationalité ou d'état civil du candidat.
Afin de garantir l'égalité des chances à toutes les personnes qualifiées, PECB fera des aménagements raisonnables pour les candidats, le cas échéant. Si un candidat a besoin d'aménagements spéciaux[2] en raison d'un handicap ou d'une condition physique particulière, il devrait en informer le revendeur/distributeur afin que celui-ci puisse prendre les dispositions nécessaires. Toute information fournie par les candidats concernant leur handicap/besoin sera traitée de manière strictement confidentielle.

Cliquez ici pour télécharger le Formulaire de demande de dispositions particulières pendant l'examen.

Plainte et appel

Toute plainte doit être déposée au plus tard 30 jours après la réception de la décision de certification (y compris la décision d'examen). PECB fournira une réponse écrite au candidat dans les 30 jours ouvrables suivant la réception de la plainte. Si la réponse de PECB n'est pas satisfaisante, le candidat a le droit de faire appel. Pour plus d'informations, consultez la Politique de plainte et d'appel de PECB.

[2] Selon le Americans with Disabilities Act (ADA), le terme « aménagement raisonnable » peut inclure : (A) rendre les installations existantes utilisées par les employés facilement accessibles et utilisables par les individus souffrant d'invalidité ; et (B) la restructuration des tâches, les horaires de travail à temps partiel ou modifiés, la réaffectation à un poste vacant, l'acquisition ou la modification d'équipement ou d'appareils, l'adaptation ou la modification appropriée des examens, du matériel de formation ou des politiques, la fourniture de personnel qualifié

Adresse
Siège social
6683, rue Jean-Talon Est, bureau 336
Montréal QC H1S 0A5
CANADA

Tel./Fax.
T : +1-844-426-7322
F : +1-844-329-7322

Centre d’aide de PECB
Visitez notre Centre d’aide pour parcourir la Foire aux questions (FAQ), consulter les manuels d’utilisation du site Web et des applications de PECB, lire les documents relatifs aux processus de PECB ou nous contacter via le système de suivi en ligne du centre d’aide.

E-mails
Examen : examination.team@pecb.com
Certification : certification.team@pecb.com
Service client : support@pecb.com