Certification de responsable de la protection des données personnelles

Présentation du corpus des connaissances pour le programme CIPM (Certified Information Privacy Manager)

La certification CIPM est composée de deux domaines : la **Gouvernance du programme de protection des données personnelles (I)** et le **Cycle de vie opérationnel du programme de protection des données personnelles (II)**.

Le **domaine I** apporte une base solide pour la gouvernance d'un programme de protection des données personnelles et définit la façon dont il peut être élaboré, mesuré et amélioré.

Le **domaine II** décrit en détail la gestion et le fonctionnement du modèle de gouvernance du programme de protection des données personnelles dans le contexte de la stratégie en matière de protection des données personnelles de l'organisation. Le domaine Cycle de vie opérationnel du programme de protection des données personnelles s'appuie sur un cadre commun accepté par l'industrie, comprenant : l'**évaluation** ou l'analyse du régime de protection des données personnelles d'une organisation ; la **protection** des actifs d'information grâce à la mise en œuvre de contrôles et de technologies de sécurité et de protection des données personnelles de pointe ; le **maintien** du programme de protection des données personnelles par le biais d'actions de communication, de formation et de gestion ; et la **réponse** aux incidents liés à la protection des données personnelles.

I. Gouvernance du programme de protection des données personnelles

A. Niveau de l'organisation

a. Créer une vision d'entreprise
   i. Acquérir des connaissances sur les approches de protection des données personnelles
   ii. Évaluer l'objectif visé
   iii. Faire adhérer le principal sponsor à cette vision

b. Établir un modèle de gouvernance des données
   1. Centralisée
   2. Décentralisée
   3. Hybride

c. Établir un programme de protection des données personnelles
    i. Définir le périmètre et la charte du programme
    ii. Identifier la source, les types et les utilisations des données personnelles au sein de l'organisation ainsi que les lois en vigueur
    iii. Développer une stratégie en matière de protection des données personnelles
        1. Alignement commercial
            a. Finaliser l'analyse de rentabilité opérationnelle pour la protection des données personnelles
            b. Identifier les parties prenantes
            c. Exploiter les fonctions clés
            d. Créer un processus pour l'interface au sein de l'organisation
            e. Aligner la culture organisationnelle et les objectif de protection des données personnelles/de la vie privée
            f. Obtenir un financement/budget pour la protection des données personnelles et l'équipe chargée de la protection des données personnelles
        2. Développer d'une stratégie de gouvernance des données pour les informations personnelles (collecte, utilisation autorisée, accès, suppression)
        3. Préparer des procédures de gestion des demandes/plaintes des personnes concernées par le traitement des données personnelles (clients, autorités de contrôle, etc.)

d. Structurer l'équipe chargée de la protection des données personnelles
    i. Établir le modèle organisationnel, les responsabilités et la forme de communication des rapports en fonction de la taille de l'organisation/entreprise
        1. Grandes organisations
            a. Directeur de la protection des données personnelles
            b. Responsable de la protection des données personnelles
            c. Analystes de la protection des données personnelles
            d. Chefs des activités de protection des données personnelles
            e. « Premiers intervenants »
        2. Petites organisations/unique délégué à la protection des données, y compris si ce n'est pas son seul emploi
    ii. Désigner un contact pour les problèmes de protection des données personnelles
    iii. Établir/adopter les mesures de compétences professionnelles

B. <u>Élaborer le cadre pour le programme de protection des données personnelles</u>

a. Développer des politiques, des normes et/ou des directives d'entreprise en matière de protection des données personnelles
b. Définir les activités du programme de protection des données personnelles
    i. Formation et sensibilisation
    ii. Surveillance et réponse à l'environnement réglementaire
    iii. Conformité de la politique interne
    iv. Inventaire de données, flux de données et classification
    v. Évaluation des risques (PIA [Privacy Impact Assessments, Analyse d'impact relative à la protection des données]) (par ex. Analyses d'impact, etc.)

vi. Procédure de violation des données en conformité avec la réglementation applicable
vii. Réparation
viii. Mise en conformité du programme, audits et contrôles de conformité inclus

C. Implémenter le cadre du programme de protection des données personnelles

a. Communiquer le cadre aux parties prenantes internes et externes
b. Garantir l'alignement permanent aux lois et règlements en vigueur afin de soutenir l'élaboration d'un cadre organisationnel pour le programme de protection des données personnelles
    i. Comprendre quand les lois et règlements nationaux s'appliquent (par ex. RGPD, CCPA)
    ii. Comprendre quand les lois et règlementations nationales s'appliquent
    iii. Appréhender les sanctions en cas de non-conformité aux réglementations applicables
    iv. Comprendre les fonctions des autorités de contrôle (par ex. autorités de contrôle de la protection des données, commissaires à la protection des données personnelles, Federal Trade Commission, etc.)
    v. Discerner les implications en matière de données personnelles dans le cas de relations commerciales avec des pays dont les lois sur la protection des données personnelles sont considérées comme inadéquates ou dans lesquels aucune loi de protection de données n'existe, ou dans le cas de l'établissement d'activités dans de tels pays
    vi. Conserver la capacité de gérer la protection des données à caractère personnel dans le monde entier
    vii. Effectuer une veille juridique mondiale au sujet de la protection des données à caractère personnel afin de suivre les évolutions
    viii. Mettre en place les accords en matière de partage international des données

D. Indicateurs

a. Identifier le public visé pour les indicateurs
b. Définir les ressources de communication des données
c. Définir les indicateurs de protection des données personnelles pour le contrôle et la gouvernance par public
    i. Indicateurs de conformité (exemples, varient selon l'organisation)
        1. Collecte (déclaration)
        2. Réponses aux enquêtes sur les personnes concernées
        3. Utilisation
        4. Conservation
        5. Divulgation à des tierces parties
        6. Incidents (violations, plaintes, enquêtes)
        7. Employés formés
        8. Indicateurs PIA
        9. Indicateurs de risque sur la protection des données personnelles
        10. Pourcentage des fonctions de l'entreprise représentées par des mécanismes de gouvernance
    ii. Suivi des tendances
    iii. Retour sur investissement du programme de protection des données personnelles
    iv. Indicateurs de résilience de l'activité
    v. Niveau de maturité du programme de protection des données personnelles
    vi. Utilisation des ressources
d. Identifier les systèmes/points de collecte d'application

II. Cycle de vie opérationnel de la protection des données personnelles

A. Évaluer votre organisation

a. Documenter la référence actuelle de votre programme de protection des données personnelles
    i. Formation et sensibilisation
    ii. Surveillance et réponse à l'environnement réglementaire
    iii. Conformité de la politique interne
    iv. Évaluation des données, systèmes et processus
        1. Faire correspondre l'inventaire de données, les flux et la classification
        2. Créer un « dossier d'autorité » des systèmes traitant des données à caractère personnel au sein de l'organisation
        3. Faire correspondre et documenter le flux de données dans les systèmes et applications
        4. Analyser et classer les types et utilisations des données
    v. Évaluation du risque (PIA, etc.)
    vi. Réponse aux incidents
    vii. Réparation
    viii. Déterminer l'état souhaité et réaliser une analyse des écarts par rapport à une réglementation ou loi applicable (notamment le RGPD)
    ix. Mise en conformité du programme, audits et contrôles de conformité inclus

b. Évaluation des sous-traitants et des fournisseurs tiers
    i. Évaluer les risques en matière de protection des données personnelles liés aux sous-traitants et aux fournisseurs tiers, à la délocalisation et à l'externalisation, notamment les règles relatives au transfert international de données
        1. Politiques en matière de protection des données à caractère personnel et de sécurité de l'information
        2. Contrôles d'accès
        3. Où les informations personnelles sont-elles conservées ?
        4. Qui a accès aux informations personnelles ?
    ii. Comprendre et tirer parti des différents types de relations
        1. Audit interne
        2. Sécurité de l'information
        3. Sécurité physique
        4. Autorité de protection des données
    iii. Évaluation du risque
        1. Type de données externalisées
        2. Emplacement des données
        3. Implications des stratégies d'informatique dans le Cloud
        4. Respect de la législation
        5. Conservation des archives
        6. Exigences contractuelles (réponse aux incidents, etc.)
        7. Établir des normes minimales pour la protection des informations
    iv. Exigences contractuelles
    v. Surveillance et audit permanents
c. Évaluations physiques
    i. Identifier le risque opérationnel
        1. Centres de données et bureaux
        2. Contrôles d'accès physiques
        3. Destruction des documents
        4. Nettoyage et élimination de supports (par ex. disques durs, clés USB/lecteurs Flash, etc.)
        5. Criminalité numérique
        6. Sécurité des appareils (par ex. appareils mobiles, Internet des objets (IoT), géolocalisation, contrôles de sécurité du disque dur des scanners et photocopieurs)
d. Fusions, acquisitions et désinvestissements
    i. Diligence raisonnable
    ii. Évaluation du risque
e. Conduire des analyses et des évaluations, selon ce qui est nécessaire ou approprié
    i. Analyse du seuil de protection des données (PTA) sur les systèmes, applications et processus
    ii. Analyses de l'impact de la protection des données (PIA)
        1. Définir un processus pour la conduite d'analyses de l'impact de la protection des données
            a. Comprendre le cycle de vie d'une PIA
            b. Incorporer une PIA dans les cycles de vie d'un système, d'un processus ou d'un produit

B. Protection

a. Cycle de vie et gouvernance des données (de la création à la suppression)
b. Pratiques de sécurité de l'information
    i. Contrôles d'accès pour des systèmes physiques et virtuels
        1. Contrôle d'accès selon le besoin de connaissance
        2. Gestion des comptes (par ex. processus de fourniture)
        3. Gestion des privilèges
    ii. Contrôles de sécurité technique
    iii. Mettre en œuvre les protections administratives adéquates
c. Prise en compte des impératifs de protection des données personnelles dès la conception (Privacy by Design)
    i. Intégrer les objectifs en matière de protection des données personnelles tout au long du cycle de vie de développement de système (SDLC)
    ii. Établir des portails de protection des données personnelles s'inscrivant dans le cadre de développement des systèmes

C. Contrôler

a. Mesure
    i. Quantifier les coûts des contrôles techniques
    ii. Gérer la conservation des données dans le respect des politiques de l'organisation
    iii. Définir les méthodes de destruction des données physiques et électroniques
    iv. Définir les rôles et responsabilités pour la gestion du partage et la divulgation des données à usage interne et externe
b. Aligner
    i. Intégrer les exigences de protection des données personnelles et la représentation aux principaux domaines à travers l'organisation
        1. Sécurité de l'information
        2. Opérations et développement TI
        3. Plan de continuité des activités (BCP) et plan de reprise après sinistre (DRP)
        4. Fusions, acquisitions et désinvestissements
        5. Ressources humaines (RH)
        6. Conformité et éthique
        7. Audit
        8. Marketing/développement commercial
        9. Relations publiques
        10. Approvisionnement
        11. Juridique et contrats
        12. Sécurité/services d'urgence
        13. Service financier
        14. Autres
c. Audit
    i. Coordonner les opérations de la protection des données personnelles avec celles d'un programme d'audit de conformité interne et externe
        1. Connaissance des processus d'audit
        2. S'aligner sur les normes industrielles
    ii. Auditer la conformité avec les politiques et les normes de protection des données personnelles
    iii. Auditer l'intégrité et la qualité des données et communiquer les résultats de l'audit aux parties prenantes
    iv. Auditer l'accès à l'information, sa modification et sa divulgation

d. Communication
    i. Sensibilisation
        1. Sensibiliser sur le programme de protection des données personnelles de l'organisation en interne et en externe
        2. Assurer la flexibilité de la politique afin d'incorporer les exigences législatives/réglementaires/de marché
        3. Élaborer des plans de communication internes et externes pour ancrer la responsabilité organisationnelle
        4. Identifier, cataloguer et conserver les documents exigeant des mises à jour en cas de changement des exigences en matière de protection des données personnelles
    ii. Formation ciblée pour les employés, la direction et les sous-traitants
        1. Politiques en matière de protection des données personnelles
        2. Pratiques de protection des données personnelles opérationnelles (par ex. instructions de fonctionnement standard), telles que
            a. Création/utilisation/conservation/suppression des données
            b. Contrôle d'accès
            c. Signalement des incidents
            d. Contacts clés
e. Surveillance
    i. Surveillance de l'environnement (par ex. systèmes, applications)
    ii. Contrôler la conformité avec les politiques établies en matière de protection des données personnelles
    iii. Surveiller les changements réglementaires et législatifs
    iv. Surveillance de la conformité (par ex. collecte, utilisation et conservation)
        1. Audit interne
        2. Autorégulation
        3. Stratégie de conservation
        4. Stratégie de sortie

D. <u>Réponse</u>

a. Demandes d'informations
    i. Accès
    ii. Réparation
    iii. Correction
    iv. Gestion de l'intégrité des données
b. Incidents liés à la protection des données personnelles
    i. Respect de la législation
        1. Éviter les préjudices
        2. Limitations en matière de collecte
        3. Responsabilité
        4. Surveillance et application
    ii. Planification de la réponse aux incidents
        1. Comprendre les rôles et responsabilités clés
            a. Identifier les parties prenantes clés de l'entreprise
                1. Sécurité de l'information
                2. Service juridique
                3. Audit
                4. Ressources humaines (RH)
                5. Service marketing
                6. Service de prospection commerciale
                7. Service communication et relations publiques
                8. Autre
            b. Établir des équipes de contrôle des incidents

2. Élaborer un plan de réponse aux incidents liés à la protection des données personnelles
3. Identifier les éléments du plan de réponse aux incidents liés à la protection des données personnelles
4. Intégrer la réponse aux incidents liés à la protection des données personnelles dans le plan de continuité de l'activité

iii. Détection des incidents
1. Définir ce qui constitue un incident lié à la protection des données personnelles
2. Identifier le processus de signalement
3. Coordonner les capacités de détection
   a. Service informatique de l'organisation
   b. Sécurité physique
   c. Ressources humaines (RH)
   d. Équipes d'enquête
   e. Fournisseurs

iv. Gestion des incidents
1. Comprendre les rôles et responsabilités clés
2. Élaborer un plan de communication pour avertir la haute direction

v. Suivre le processus de réponse aux incidents afin de garantir le respect des exigences juridictionnelles, mondiales et commerciales
1. Engager une équipe chargée de la protection des données personnelles
2. Examiner les faits
3. Réaliser une analyse
4. Déterminer les mesures à prendre (contenir, communiquer, etc.)
5. Exécution
6. Surveillance
7. Examiner et appliquer les leçons apprises

vi. Identifier les techniques de réduction des incidents

vii. Identificateurs d'incidents - quantifier le coût d'un incident lié à la protection des données personnelles