Guide Pratique

L'audit des risques d'atteinte à la vie privée

2e édition

JUILLET 2012

ifaci
institut français de l'audit et du contrôle internes

The Institute of Internal Auditors

SOMMAIRE

I. Résumé 4

II. Introduction 6

III. Cadre de référence et principes de protection de la vie privée 11

IV. Protection de la vie privée - Entreprises, organisations à but non lucratif et entités publiques 15

V. Auditer la protection de la vie privée 20

VI. 12 questions que le responsable de l'audit interne devrait se poser concernant la protection de la vie privée 32

VII. Annexe 33

ISBN : *978-2-915042-52-8*

Toute représentation ou reproduction, intégrale ou partielle, faite sans le consentement de l'auteur, ou de ses ayants droits, ou ayants cause, est illicite (loi du 11 mars 1957, alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal.

I. RÉSUMÉ

Pourquoi est-il important de protéger la vie privée ?

La protection des données personnelles relatives à leurs clients, leurs collaborateurs et leurs partenaires commerciaux est actuellement l'un des principaux aspects de la gestion des risques au sein des organisations. Les consommateurs sont préoccupés par la façon dont les organisations utilisent et protègent ces informations. Les investisseurs et le management s'attachent à répondre aux besoins et aux attentes de leurs clients, de leurs partenaires externes et de leur personnel. Ils veillent également à respecter les engagements contractuels ainsi que la législation et la réglementation en vigueur concernant le respect de la vie privée et la sécurité.

La protection de la vie privée est un impératif global. De nombreux pays ont adopté une législation qui régit l'utilisation, ainsi que l'exportation à l'extérieur des frontières, des données personnelles. Pour opérer efficacement dans cet environnement, les entreprises doivent comprendre cette législation et s'y conformer. La Loi sur la protection des données personnelles et les documents électroniques (LPRPDÉ) au Canada, la Directive sur la protection des données personnelles de l'Union européenne (UE) et les lois adoptées par l'Australie, le Japon et la Nouvelle-Zélande en sont des exemples notables. Aux États-Unis, la législation sur la protection de la vie privée se compose notamment du Gramm-Leach Bliley Act (GLBA) dans le secteur des services financiers et du Health Insurance Portability and Accountability Act (HIPAA) dans le secteur de la santé.

L'actualité est riche d'exemples d'atteintes à la sécurité, qui se traduisent par la perte ou la divulgation de données personnelles. Un grand nombre d'organisations externalisent des processus et des applications qui contiennent des données personnelles, et utilisent des technologies nouvelles, pouvant accroître leur profil de risque d'atteinte à la vie privée. Les parties prenantes telles que les Conseils[1], les comités d'audit et d'autres instances de surveillance souhaitent obtenir l'assurance que les processus de leur organisation protègent bien les données personnelles.

Les avantages d'une bonne gouvernance et maîtrise des risques d'atteinte à la vie privée

Une bonne gouvernance impose de recenser les risques significatifs auxquels est exposée une organisation - mauvaise utilisation, fuite ou perte de données personnelles - et de faire en sorte que des contrôles appropriés soient mis en place pour maîtriser ces risques.
Pour les entreprises, une bonne maîtrise des risques d'atteinte à la vie privée permet :

- de faire face au risque d'image et de réputation,
- de sécuriser les données importantes, relatives aux clients, au personnel, aux partenaires externes,
- de générer un avantage compétitif sur le marché,
- de se conformer à la législation et à la réglementation en vigueur,
- d'accroître leur notoriété, d'inspirer confiance et donc d'augmenter leur valeur boursière.

Pour le secteur public ou les organisations à but non lucratif, une bonne maîtrise des risques d'atteinte à la vie privée permet également :

[1] Le terme « Conseil » utilisé dans ce guide correspond à la définition du glossaire des *Normes Internationales pour la Pratique Professionnelles de l'audit interne*, à savoir : « Le niveau le plus élevé des organes de gouvernance, responsable du pilotage, et/ou de la surveillance des activités et de la gestion de l'organisation. Habituellement, le Conseil (par exemple, un conseil d'administration, un conseil de surveillance ou un organe délibérant) comprend des administrateurs indépendants. Si une telle instance n'existe pas, le terme « Conseil »», utilisé dans les Normes, peut désigner le dirigeant de l'organisation. Le terme « Conseil » peut renvoyer au comité d'audit auquel l'organe de gouvernance a délégué certaines fonctions. »

- de garder la confiance des individus (quelle que soit leur nationalité),
- de préserver les relations avec les donateurs qui financent les organismes à but non lucratif, en respectant la confidentialité de leurs activités.

Assurer le maintien de pratiques efficaces

La plupart des organisations admettent la nécessité d'instaurer de bonnes pratiques pour protéger la vie privée. L'instauration de telles pratiques constitue toutefois un enjeu délicat. En effet, avec la multiplication des technologies permettant de collecter, d'utiliser, de communiquer, de conserver ou de détruire de grands volumes de données personnelles et d'externaliser entièrement des processus informatiques dans des sites nationaux et à l'étranger, les organisations peuvent avoir du mal à déterminer où ces données sont stockées, comment elles sont protégées, qui y a accès et comment leur utilisation est sécurisée. Les évolutions rapides de la technologie, telles que l'informatique mobile, les réseaux sociaux, l'identification par radiofréquence (RFID) et les services géodépendants, ont accru l'accessibilité aux données personnelles relatives aux clients, au personnel et à d'autres individus. Ce bouleversement a été plus rapide que l'évolution du cadre juridique, des normes et pratiques des secteurs et des organisations, nécessaires à la protection de cet actif précieux. De surcroît, les responsabilités afférentes à la gestion d'un dispositif de protection de la vie privée ne sont pas toujours clairement définies, car souvent disséminées dans toute l'organisation. Il peut en résulter des incohérences et de l'incertitude concernant la mise en place et l'efficacité des pratiques destinées à protéger la vie privée.

II. INTRODUCTION

Comme exposé dans la Modalité Pratique d'Application de l'IIA 2130.A1-2, « L'évaluation du dispositif mis en place par l'organisation pour protéger la vie privée », l'audit interne peut contribuer à une bonne gouvernance et à l'amélioration du management des risques en évaluant l'adéquation de l'identification des risques réalisée par le management en ce qui concerne la protection de la vie privée ainsi que celle des contrôles mis en place pour atténuer ces risques à un niveau acceptable. Certains des avantages liés à la réalisation d'une mission d'audit de la protection de la vie privée sont exposés ci-après.

Avantages découlant d'une mission d'audit de la protection de la vie privée

- Contribuer au respect de la législation et de la réglementation en vigueur.
- Mesurer et contribuer à améliorer la conformité au dispositif de protection des données de l'organisation.
- Identifier les incohérences potentielles entre les politiques et les pratiques.
- Accroître la sensibilisation du management et du personnel à l'importance de la protection des données.
- Fournir des informations pour réaliser une évaluation du dispositif de protection des données.
- Donner une assurance concernant le risque de réputation.
- Améliorer les procédures de réponse aux plaintes concernant la vie privée.

Ce guide pratique complète et développe les points abordés dans la Modalité Pratique d'Application 2130.A1-2. Il informe le responsable de l'audit interne et les auditeurs internes sur les risques d'atteinte à la vie privée auxquels l'organisation est confrontée lorsqu'elle collecte, utilise, conserve, divulgue et détruit des données personnelles. Il présente une vue d'ensemble des principaux référentiels régissant la protection de la vie privée, afin d'aider le lecteur à comprendre les concepts de base et à trouver les bonnes sources de recommandations supplémentaires concernant les attentes et les pratiques efficaces dans divers environnements. Ce guide montre également comment les auditeurs internes peuvent évaluer la protection de la vie privée.

Qu'est-ce que la protection de la vie privée ?

La protection de la vie privée peut avoir plusieurs significations selon les contextes. Il est possible de l'analyser sous un angle descriptif ou normatif ou d'un point de vue moral ou juridique. Elle peut faire référence à la volonté d'échapper à l'attention, à l'observation, à la surveillance d'autrui. Elle peut concerner le caractère privé d'une communication, comme d'une information. Dans sa forme la plus simple, la protection de la vie privée peut être définie comme « le droit d'avoir la paix ».[2]

Dans l'environnement des entreprises, les définitions de la protection de la vie privée diffèrent considérablement en fonction du pays, de la culture, de la situation politique et du cadre juridique. Dans de nombreux pays, la protection de la vie privée est étroitement liée à la protection des données. Pour les organisations, la façon dont elles définissent la protection de la vie privée revêt une importance particulière. Qu'il s'agisse des définitions données dans la Figure 1, ou que la protection de la vie privée soit simplement considérée comme la protection de la collecte, du stockage, du traitement, de la diffusion et de la destruction de données personnelles, ces multiples définitions peuvent être utilisées par toute organisation pour orienter sa propre démarche de protection de la vie privée.

[2] The Right to Privacy / Warren, Brandeis. – in Harvard Law Review, Vol. IV 15 décembre 1890, N°5.

Figure 1 – Définitions de la protection de la vie privée

« La protection de la vie privée est la protection des données personnelles et est considérée comme un droit fondamental. »
– Lignes directrices de l'Organisation pour la coopération et le développement économique (OCDE), 1980

« Les États membres assurent […], la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données personnelles. »
– Directive de l'Union européenne (UE), 1995

« Des droits et obligations des individus et des organismes quant à la collecte, à l'utilisation, à la divulgation et à la conservation des données personnelles. »
– American Institute of Certified Public Accountants (AICPA) / Institut canadien des comptables agréés (ICCA), 2009

La protection de la vie privée porte souvent sur les données personnelles concernant un individu et sa capacité à :

- Savoir comment ces informations sont gérées.
- Contrôler les informations collectées.
- Contrôler l'usage qui en est fait.
- Contrôler l'identité de celui qui a accès à ces informations.
- Modifier ou supprimer ces informations.

Les données personnelles sont des données qui peuvent se rapporter à un individu ou qui peuvent être utilisées pour l'identifier, directement ou indirectement. Certaines données personnelles sont considérés comme sensibles, comme le décrit la Figure 2. Les données personnelles peuvent être préservées grâce à un traitement et à une protection adéquats.

Figure 2 - Exemples de données personnelles et sensibles

DONNÉES PERSONNELLES	• Nom • Sexe • Date de naissance • Adresse postale • Numéro de téléphone personnel • Adresse électronique personnelle • Numéro d'identification (par exemple carte d'identité, numéro de sécurité sociale) • Identifiant biométrique • Photographie ou vidéo permettant d'identifier un individu • Informations sur le comportement (par exemple dans un système de gestion de la relation client)
DONNÉES MÉDICALES SENSIBLES	• Dossiers médicaux • Informations sur le bénéficiaire d'un régime de couverture médicale • Informations sur la santé physique ou mentale • Traitements médicaux ou toute information recueillie pendant un traitement médical
DONNÉES FINANCIÈRES SENSIBLES	• Coordonnées bancaires (par exemple numéros de compte, cartes de crédit) • Historique financier • Informations sur la rémunération
AUTRES DONNÉES SENSIBLES	• Origine raciale ou ethnique • Convictions religieuses ou philosophiques • Opinions politiques • Adhésion à un syndicat • Procès et poursuites au civil • Combinaison de certaines informations

Bien que n'étant pas par nature à caractère personnel, certaines informations deviennent des données personnelles sensibles lorsqu'elles sont combinées à d'autres informations. Ces données personnelles sensibles requièrent généralement un degré de protection et de vigilance supérieur. Pour une organisation, la mise en œuvre d'une méthode de classification des données, incluant les données personnelles, constitue un bon moyen d'atteindre ce niveau de protection et de vigilance. Elle s'accompagne de recommandations contribuant à l'instauration et au maintien de pratiques homogènes dans toute l'organisation, en fonction de la nature des données.

Protection de la vie privée

La protection de la vie privée peut être considérée comme un processus consistant à concilier la vie privée et de multiples intérêts concurrentiels. Afin de réduire le plus possible les intrusions, de garantir l'équité et de respecter les attentes légitimes et réalistes à l'égard de la protection de la vie privée, l'ensemble des principes qui régissent le traitement des données personnelles, ainsi que les fonctions correspondantes (Figure 3) ont évolué au cours des décennies. Ces principes englobent divers concepts, tels que la qualité, l'intégrité et la limitation de l'utilisation des données, et des principes liés aux procédures, comme le consentement et les droits d'accès.

Figure 3 – Les parties prenantes

Lors de la mise en œuvre d'un dispositif relatif à la protection de la vie privée, il est nécessaire de prendre en compte les principales parties prenantes :

La personne concernée – L'individu dont les données personnelles sont collectées, utilisées, divulguées, conservées et détruites.

Le contrôleur de la protection des données – L'organisation qui contrôle l'accès aux données personnelles et leur traitement.

Le responsable des données personnelles – La personne qui, au sein d'une organisation, est chargée de la surveillance/du contrôle du respect de la vie privée et qui est l'interlocuteur dans ce domaine.

Le commissaire à la protection de la vie privée – Un organisme public de surveillance.

Les prestataires de services – Dans les cas où le traitement des données personnelles fait intervenir des tiers.

La façon dont une organisation gère les données personnelles (de ses clients, de ses collaborateurs et de ses partenaires externes) qu'elle collecte, utilise, conserve, protège, divulgue et détruit, se trouve au cœur du problème de la protection de la vie privée dans l'entreprise. À la suite d'incidents récents, comme l'usurpation d'identité, le détournement de données personnelles, ou la violation des principes de protection de la vie privée, les autorités de réglementation et les associations de consommateurs poussent les organisations à mettre en place des dispositifs de contrôle de leur gestion de l'information en conformité avec la protection de la vie privée et la sécurité des données personnelles.

Risques d'atteinte à la vie privée

Pour les entreprises, les pouvoirs publics et les organismes à but non lucratif, la protection de la vie privée relève de la maîtrise des risques. Les enquêtes continuent de montrer que les consommateurs et les citoyens se préoccupent de l'usage que font les organisations des données personnelles. Si la direction et les contrôleurs de la protection des données d'une entreprise ne gèrent pas bien la protection de ces informations, il en découle de nombreux risques pour l'organisation, et notamment :

- Un risque d'atteinte à son image et à sa réputation.
- Un risque de manque à gagner ou de perte pour les investisseurs.
- Une responsabilité juridique et des sanctions professionnelles ou réglementaires.
- Des accusations de tromperie.
- Une méfiance des clients, des citoyens ou du personnel.
- Une perte de clientèle et de chiffre d'affaires.
- Une dégradation des relations d'affaires.

Contrôles du dispositif de protection de la vie privée

Pour que l'organisation puisse maîtriser les risques d'atteinte à la vie privée auxquels elle est confrontée, il est essentiel que le Conseil et la direction générale instaurent une gouvernance et une surveillance appropriées. Les autres contrôles fondamentaux relatifs à la protection de la vie privée comprennent la détermination d'objectifs, l'élaboration de politiques et procédures et la mise en place de dispositifs de surveillance et d'amélioration. De plus, afin de mettre en évidence ses points faibles, l'organisation devrait évaluer la conformité de ses pratiques de protection de la vie privée et de gestion des données, en les confrontant à ses propres politiques internes, à la législation et la réglementation, ainsi qu'aux bonnes pratiques en la matière.

Une gestion efficace de la protection de la vie privée intègre :

- Gouvernance et « devoir de rendre compte » en matière de protection de la vie privée.
- Répartition des rôles et des responsabilités.
- Déclaration de confidentialité.
- Diffusion de politiques et procédures écrites sur la collecte, l'utilisation, la divulgation, la conservation et la destruction des données personnelles.
- Mise en œuvre de mesures relevant de la sécurité de l'information.
- Formation et information du personnel.
- Évaluations des risques d'atteinte à la vie privée et modèles de maturité.
- Pilotage et audit.
- Conformité à la législation et à la réglementation.
- Recensement des types de données personnelles et de leurs utilisations.
- Classification des données.
- Dispositifs de gestion des risques d'atteinte à la vie privée liés au développement de systèmes ou à la création et modification de processus opérationnels.
- Contrôles relatifs aux prestataires externes.
- Mise en place de consignes pour la gestion des incidents liés à la violation des données personnelles.
- Programmation des mesures correctives.

La MPA 2130.A1-2 recommande également que les auditeurs internes contribuent à une bonne gouvernance et à la transparence et aident l'organisation à atteindre ses objectifs de protection de la vie privée en jouant un rôle d'assurance et de conseil.

III. CADRE DE RÉFÉRENCE ET PRINCIPES DE PROTECTION DE LA VIE PRIVÉE

3.1 De nombreuses réglementations et des attentes complexes

Depuis la fin des années 1960, de nombreux cadres de référence et principes régissant la protection de la vie privée ont été élaborés et publiés. Les cadres les plus utiles sont fondés sur des principes, et couvrent généralement les droits des individus à la protection de la vie privée. Ils tentent également de tenir compte des droits des organisations, des entreprises et des économies à opérer de manière efficace.

La législation et la réglementation relatives à la protection de la vie privée sont variées, de plus en plus complexes et leur nombre augmente rapidement par secteur, régulateur local, pays, voire région. Des cadres solides peuvent aider une organisation à renforcer sa conformité et à avoir une meilleure articulation des principes admis en matière de protection de la vie privée.

Les besoins et la réglementation concernant la protection de la vie privée ont pris une importance accrue. Conscientes de l'importance des besoins dans le domaine de la protection de la vie privée, les Nations Unies ont officiellement parrainé des études dès 1968 et peu après, élaboré des principes fondés sur les droits de l'Homme. Plus récemment, l'attention s'est tournée vers l'élaboration de principes « communément admis » de protection de la vie privée afin de contribuer à gérer d'éventuels conflits futurs. Par exemple, les pouvoirs publics doivent protéger les individus, tout en protégeant la société des menaces criminelles ou terroristes en effectuant une surveillance préventive et en menant des investigations à l'aide des traces d'informations.

Différents cadres de référence et principes récents relatifs à la protection de la vie privée sont utiles pour ceux qui :

- Supervisent et surveillent les programmes de protection de la vie privée et de sécurité.
- Mettent en œuvre et gèrent la politique de protection de la vie privée au sein d'une organisation.
- Mettent en œuvre et gèrent la politique de sécurité au sein d'une organisation.
- Supervisent et gèrent les risques et la conformité au sein d'une organisation.
- Évaluent la conformité et auditent les dispositifs de protection de la vie privée et de sécurité.
- Régulent la protection de la vie privée.

La Figure 4 présente des exemples de cadres législatifs, réglementaires ou professionnels, ainsi que les principes communs contenus dans ces cadres.

Figure 4 – Exemples de principes inscrits dans des cadres de référence régissant la protection de la vie privée[3]

AICPA/CICA - PRINCIPES DE PROTECTION DE LA VIE PRIVÉE COMMUNÉMENT ADMIS	LOI AUSTRALIENNE SUR LA PROTECTION DE LA VIE PRIVÉE	LOI CANADIENNE PIPEDA	DIRECTIVE DE L'UE	LOI JAPONAISE SUR LA PROTECTION DES DONNÉES PERSONNELLES	LIGNES DIRECTRICES DE L'OCDE	*FEDERAL TRADE COMMISSION* DES ÉTATS-UNIS
Gestion		Responsabilité / Devoir de rendre compte	Déclaration	Désignation de la responsabilité	Responsabilité / Devoir de rendre compte	
Avis	Transparence	Identification des objectifs, transparence	Informations à transmettre à la personne concernée	Avis, publication de l'objectif de l'utilisation	Définition de l'objectif, transparence	Avis
Choix et consentement	Utilisation et divulgation	Consentement	Critères justifiant le traitement des données, droit de contestation de la personne concernée	Consentement	Limitation de la collecte	Choix
Collecte	Collecte, données sensibles, anonymat	Limitation de la collecte	Principes relatifs à la qualité des données, aux exemptions et aux limitations	Pas de méthode de collecte inéquitable	Limitation de la collecte (dont le consentement)	
Utilisation, conservation et destruction	Identifiants, utilisation et divulgation	Limitation de l'utilisation, de la divulgation et la conservation	Justification du traitement des données ; catégories spéciales de traitement ; principes relatifs à la qualité des données, aux exemptions et aux limitations ; droit de contestation de la personne concernée	L'objectif de l'utilisation ne sort pas du champ prévu	Limitation de l'utilisation (dont limitation de la divulgation	

[3] Adapté à partir de la comparaison des concepts internationaux relatifs à la protection de la vie privée réalisée par l'AICPA/CICA

AICPA/CICA - PRINCIPES DE PROTECTION DE LA VIE PRIVÉE COMMUNÉMENT ADMIS	LOI AUSTRALIENNE SUR LA PROTECTION DE LA VIE PRIVÉE	LOI CANADIENNE PIPEDA	DIRECTIVE DE L'UE	LOI JAPONAISE SUR LA PROTECTION DES DONNÉES PERSONNELLES	LIGNES DIRECTRICES DE L'OCDE	*FEDERAL TRADE COMMISSION* DES ÉTATS-UNIS
Accès	Accès et modification	Accès individuel	Droit d'accès de la personne concernée aux données	Accès et modification	Participation individuelle	
Divulgation à des tiers	Utilisation et divulgation, flux de données transfrontières	Utilisation et divulgation, flux de données transfrontières	Transfert de données personnelles à des pays étrangers	Transfert de données personnelles, clause de désinscription (opt-out), délégation, fusion, utilisation conjointe	Limitation de l'utilisation (dont limitation de la divulgation)	
Sécurité de la vie privée	Sécurité des données	Garde-fous	Confidentialité et sécurité du traitement	Mesures de contrôle de la sécurité	Garde-fous relatifs à la sécurité	Sécurité
Qualité	Qualité des données	Exactitude	Principes relatifs à la qualité des données	Intégrité des données	Qualité des données	Intégrité
Surveillance et mise en application	Mise en application par l'*Office of the Privacy Commissioner*	Plaintes relatives à la conformité	Recours judiciaires, responsabilité et sanctions, codes de conduite, organe de supervision et groupe de travail sur la protection des individus à l'égard du traitement des données personnelles	Mise en application	Participation individuelle (dont plaintes relatives à la conformité)	Mise en application

3.2 Quel cadre de référence de protection de la vie privée utiliser ?

Il est essentiel que la direction consulte son conseiller juridique sur la législation et la réglementation relative à la protection de la vie privée pour coordonner la façon dont le cadre de référence de protection de la vie privée et l'approche en matière de conformité sont développés, évalués et contrôlés.

Les cadres exposés dans la Figure 4 partagent de nombreux principes. En général, ces cadres sont conçus pour contribuer à la mise en œuvre de principes énoncés par l'autorité compétente. Certains sont applicables à l'échelle internationale, régionale ou nationale, tandis que d'autres concernent un secteur, un régulateur ou un éventail spécifique de besoins professionnels ou commerciaux. D'un point de vue technique et juridique, les cadres vont d'une législation transnationale et nationale aux organismes non gouvernementaux, et peuvent être d'application obligatoire ou facultative. En outre, ils émanent des normalisateurs professionnels tels que l'Organisation internationale de normalisation (ISO) et des instances telles que le *Payment Card Industry* (PCI) *Security Standards Council*.

Utiliser plusieurs sources

L'identification d'un cadre de référence de protection de la vie privée qui conviendrait à une organisation spécifique dépend de nombreux facteurs, et ne sera donc pas abordée dans ce guide. La législation et la réglementation sur la protection de la vie privée dictent et influencent souvent le cadre qui sera adopté par l'organisation. Dans d'autres situations, les personnes physiques et les organisations peuvent faire preuve de bons sens, suivre la législation ou décider de la manière dont ils prévoient de répondre aux préoccupations potentielles de groupes ou d'individus concernant la protection de la vie privée. Dans tous les cas, il est primordial de solliciter l'avis d'un conseiller juridique lors de l'élaboration ou de l'adoption d'un cadre de protection de la vie privée.

IV. PROTECTION DE LA VIE PRIVÉE – ENTREPRISES, ORGANISATIONS À BUT NON LUCRATIF ET ENTITÉS PUBLIQUES

Les organisations commerciales comptent trois principaux groupes de parties prenantes : les propriétaires / prêteurs, les salariés / collaborateurs et les clients / le public. Les organisations à but non lucratif ont des salariés / collaborateurs et des conseils de surveillance pour gérer leurs activités. Les entités publiques sont au service des citoyens et des étrangers et peuvent également avoir des clients. Dans tous les cas, une bonne gouvernance nécessite que les organisations tiennent compte des risques d'atteinte à la vie privée, et ce même lorsqu'ils sont basés sur des motifs divergents - des droits légaux à la simple bonne pratique.

4.1 Impacts de la protection de la vie privée

Les organisations ont recours aux données personnelles d'un individu dans le cadre de différentes activités : études de marché, classification des clients, gestion de droits, marketing direct, vente de données. Ces données peuvent également intéresser l'entourage, les amis, la famille et le réseau professionnel de l'individu.

Des données personnelles peuvent également être collectées et utilisées par l'État ou par les autorités gouvernementales de pays étrangers, des concurrents, des salariés mécontents, des pirates informatiques, des cyber-terroristes, des saboteurs, des usurpateurs d'identité, etc. En raison des menaces qui pèsent sur les personnes concernées, les organisations doivent protéger efficacement les données personnelles (qu'elles gèrent) afin d'éviter tout dommage ainsi que tout litige pouvant en découler.

4.2 Menaces liées à la protection de la vie privée

Les menaces et les risques d'atteinte à la vie privée peuvent être analysés en utilisant une approche multi-couche qui décrit l'organisation, ses parties prenantes et les individus.

Menaces pesant sur les organisations

Les organisations sont confrontées à des menaces et des risques tangibles. Elles ressentent presque immédiatement l'impact des manquements à la protection de la vie privée, celui-ci étant souvent abondamment abordé par les médias, les organes de supervision et les systèmes de protection de la vie privée.

Les menaces qui pèsent sur son fonctionnement restreignent la capacité d'une organisation à atteindre ses objectifs. Elles peuvent perturber ses activités et sont sources d'inefficience ou d'inefficacité. Les risques qui pèsent sur la réputation d'une organisation limitent potentiellement sa capacité future à élargir son portefeuille de clients, à répondre aux besoins de ses clients ou aux attentes des citoyens.
Cependant, si une organisation gère bien ces menaces et ces risques, elle peut en tirer un avantage compétitif. Ce sont les répercussions financières pour l'organisation qui importent le plus aux parties prenantes, dans la mesure où elles proviennent principalement des entraves à l'activité et des atteintes à la réputation dues aux risques d'atteinte à la vie privée. Des risques supplémentaires d'atteinte à la vie privée apparaissent lorsqu'une organisation procède à l'externalisation totale ou partielle de ses activités, en regroupe ou en arrête certaines, ou lorsqu'elle embauche, gère ou licencie du personnel. D'autres faiblesses des pratiques commerciales et des contrôles qui augmentent potentiellement le profil de risque de l'organisation sont détaillées dans la Figure 5.

Figure 5 – Faiblesses des contrôles de protection de la vie privée lors du traitement de données personnelles

- Débordement au niveau de la collecte.
- Informations tronquées.
- Données altérées.
- Informations obsolètes.
- Contrôles d'accès inopérant.
- Partage excessif des données.
- Traitement incorrect.
- Conservation des données personnelles plus longtemps que nécessaire.

Menaces pesant sur les parties prenantes

Même si des pratiques et des contrôles de protection de la vie privée excessifs peuvent restreindre l'efficience d'une organisation, tant pour ses processus internes que vis-à-vis de l'extérieur, les parties prenantes sont généralement confrontées à des risques bien plus grands, résultant d'une réputation ternie ou de litiges, et qui réduisent donc la valeur et la rentabilité de leur investissement. La mise en œuvre de pratiques adaptées à la protection de la vie privée permet donc de sécuriser la valeur des investissements dans une entreprise.

Menaces pesant sur les individus

Les individus sont souvent confrontés aux conséquences directes des menaces d'atteinte à leur vie privée : il arrive qu'ils soient victimes d'usurpation d'identité, doivent supporter des coûts supplémentaires, qu'ils soient victimes de discrimination, ou qu'ils n'aient pas vraiment le choix lorsqu'ils communiquent leurs données personnelles à des entités publiques, des institutions financières, des distributeurs, des fournisseurs ou des prestataires de services.

Par exemple, lorsqu'un individu recherche un nouvel emploi, il adresse un *curriculum vitae* (CV) détaillé à des portails, des cabinets-conseil ou des employeurs potentiels, qui sont susceptibles d'utiliser ces données personnelles à d'autres fins que celles prévues, sans qu'il y consente ou le sache. Parfois, des données personnelles sont traitées au moyen de techniques de sélection et de profilage, qui peuvent être intrusives, malhonnêtes et non fiables, ou avoir des conséquences néfastes pour la personne concernée.

4.3 Problématiques sectorielles relatives à la vie privée

Il est crucial que les auditeurs internes comprennent bien le cadre juridique dans lequel l'organisation opère, et qu'ils tiennent compte de l'ensemble de la législation, de la réglementation et des autres recommandations sectorielles. Ce faisant, il importe également que l'auditeur interne fasse appel au conseiller juridique de l'entreprise. Cette section donne des exemples de problèmes potentiels liés à la protection de la vie privée, par domaine.

L'État et le citoyen

Diverses entités publiques collectent, stockent et échangent des données personnelles. Les personnes concernées et les contrôleurs de la protection des données sont confrontés en permanence à la menace d'une utilisation abusive, de perte ou de vol de vastes fichiers publics.

Une réglementation applicable au secteur public définit comment traiter les données personnelles. Dans de nombreux pays, des lois-cadres existent pour les entités publiques à différents niveaux. D'autres pays ont établi des règles qui s'appliquent au cas par cas. En conséquence, les auditeurs du secteur public doivent se concentrer sur un large éventail de documents / bases

et de programmes : cadastres, listes électorales, recensements et sondages d'opinion, archives fiscales, fichiers de la sécurité nationale, informations collectées pour les programmes de protection sociale et le travail social, pour le système éducatif et par la police.

Vie collective et services sociaux

De nombreuses entités stockent et traitent des données sensibles. C'est ainsi que pour mener leurs activités, nombre d'institutions de protection sociale (assureurs, programmes d'aide publics, programmes de travail social et autres organismes à but non lucratif) gèrent de vastes bases de données sensibles. Dans bien des cas, la réglementation en vigueur pour les secteurs public ou privé peut être appliquée. Néanmoins, certaines institutions, telles que les églises, peuvent en être exemptées, ce qui est susceptible d'affaiblir le dispositif de protection de la vie privée. Des données sensibles sont stockées et traitées dans de nombreuses situations. Les groupes risquent fort de perdre la confiance de leurs membres si elles traitent les données personnelles sans porter l'attention qui s'impose à la confidentialité.

Les systèmes de protection sociale et d'administration publique peuvent engendrer une exposition supplémentaire à des risques, en opérant de manière indue ou excessive une intégration (par rapprochement ou juxtaposition) de données personnelles provenant de diverses sources. Souvent, des règles, des lois ou des accords spécifiques déterminent dans quelles circonstances le rapprochement ou le partage de ces données est légitime. Le détournement d'usage d'identifiants constitue un autre risque en matière d'atteinte à la vie privée qui peut se réaliser via la récupération et le rapprochement de données, ainsi que la manipulation ou l'usurpation d'identité.

Services financiers

Les prestataires de services financiers, comme les banques, les émetteurs de cartes de paiement, les fonds et les assureurs, gèrent de très nombreuses données personnelles sensibles, qui ont notamment trait à l'évaluation de la solvabilité, au revenu, aux habitudes de dépenses, au lieu de résidence et aux antécédents de crédit. C'est pourquoi, il existe un vaste arsenal réglementaire, et un large éventail d'organes de supervision susceptibles d'intervenir.

Marketing et distribution

Les domaines du marketing et de la distribution collectent, utilisent et diffusent à grande échelle des données personnelles. Les informations qu'ils gèrent vont de listes d'adresses à des profils de consommation détaillés, en passant par des renseignements financiers et des historiques d'achats.
Par exemple, lorsqu'un individu fait un achat, son compte peut être débité immédiatement, et un relevé indique la date, l'heure et le lieu de l'achat, ainsi que le fournisseur. Lorsque vous achetez ou que vous surfez sur Internet, les distributeurs et les fournisseurs peuvent utiliser des techniques *marketing* de suivi pour contrôler et collecter des données personnelles. De plus, des mécanismes de traçage et de marquage, tels que des technologies d'identification par radiofréquence, commencent à apparaître, ce qui pose des problèmes de protection de la vie privée et notamment la capacité de suivre une personne à la trace.

De nombreuses sources recueillent des données personnelles, notamment les points de vente, les sources publiques et individuelles, les courtiers en information et d'autres organisations. Ces données peuvent être utilisées pour identifier et contacter des clients

potentiels, pour définir des groupes homogènes de consommateurs grâce à l'exploitation statistique des connaissances à partir d'une base de données ou pour élaborer des profils détaillés qui serviront à cibler les besoins et centres d'intérêt individuels.
Les associations sectorielles proposent divers codes de conduite à l'intention des sociétés de marketing. Ainsi, en Australie, l'*Australian Direct Marketing Association* (ADMA) a rédigé un code d'autorégulation comprenant 10 principes de protection de la vie privée que tous ses membres doivent prendre en compte et respecter.

Communication et médias

Dans le domaine de la communication et des médias, la protection de la vie privée englobe la capacité à préserver la confidentialité des données personnelles, au même titre que la liberté d'accès aux médias et aux canaux de communication. De plus, les données personnelles qui sont saisies dans des bases de clients, d'abonnés et d'emprunteurs peuvent être utilisées pour déterminer les préférences et le profil d'individus. En les combinant avec des données relatives à des transactions, on crée un fichier de données personnelles portant sur les habitudes d'achat et d'utilisation des services, notamment sur les interlocuteurs, la date, le lieu et le contenu. Il peut en résulter des pratiques telles que des courriers non sollicités *(spams)*, l'écoute clandestine, la divulgation imprévue de communications et de contenus ou une surveillance excessive par l'État.

Services collectifs, transports et déplacements

Les systèmes de services aux collectivités et de transports publics sont sophistiqués et fonctionnent en réseau. Par exemple, chaque passage d'un individu à un péage est enregistré par identification par radiofréquence, le numéro de la plaque d'immatriculation de son véhicule est enregistré par la société de péage et sa carte de paiement débitée du montant à payer. Cinq minutes plus tard, un autre système enregistre le véhicule à l'entrée d'un parc de stationnement. Ces systèmes intégrés peuvent permettre d'élaborer des profils détaillés d'individus, en procédant au rapprochement des données émanant des dispositifs de circulation et de contrôle d'accès avec des informations supplémentaires relatives à d'autres transactions. De nombreux pays estiment qu'ils devront instaurer des mesures de sécurité supplémentaires ou invoquer la Constitution pour éviter la collecte excessive de données personnelles et, ainsi, protéger la vie privée des citoyens et des consommateurs.

Santé et recherche

Le secteur de la santé requiert et collecte des informations sensibles sur les patients. La recherche clinique, les services et les tests médicaux, ainsi que la gestion des maladies, requièrent des données personnelles. Aux États-Unis, la loi HIPAA protège les données personnelles des patients. Elle s'applique aux régimes de couverture maladie, aux organismes de centralisation de données sanitaires, aux prestataires de services de santé et aux employeurs. D'autres pays ont voté des lois analogues. La législation comporte des dispositions clés telles que des restrictions s'appliquant à l'utilisation et à la divulgation de données personnelles, et instaure des garde-fous administratifs, physiques et techniques pour éviter une utilisation ou une divulgation volontaire ou involontaire. D'autres pays ont mis en place un ensemble de lois similaires.

Activités internationales

Nombre de textes législatifs et réglementaires interdisent de faire sortir des données personnelles du territoire sur lequel ils s'appliquent. Ces règles répondent aux inquiétudes suscitées par la perte de contrôle sur des données personnelles transférées à une autre juridiction. Si ces informations sont mal gérées, les organisations qui

transfèrent de telles informations seront confrontées à des tracasseries considérables, verront leur réputation entachée ou subiront des pertes financières.
De graves questions se posent donc dans un univers de systèmes en réseau, où l'information franchit les frontières au sein d'une même organisation, est traitée ou stockée dans le *cloud* - qui traverse potentiellement les frontières et les juridictions - ou est partagée ou échangée avec des partenaires commerciaux qui utilisent et traitent des données personnelles au niveau transnational.

V. AUDITER LA PROTECTION DE LA VIE PRIVÉE

Une mission concernant le dispositif de protection de la vie privée suit les étapes classiques d'une mission d'audit (évaluation des risques, planification, réalisation et communication des résultats). Cependant, le responsable de l'audit interne devra également tenir compte d'autres aspects, comme la constatation d'éventuelles atteintes à la vie privée, la gestion du personnel, les questions de conservation des données et une évaluation de la protection de la vie privée par d'autres prestataires d'assurance. La plupart de ces aspects sont couverts par les pratiques professionnelles de l'audit interne et de l'audit externe. Ce chapitre en expose les principaux enjeux et les méthodes existantes.

Il est important pour l'auditeur de communiquer avec un conseiller juridique dès le début de la mission afin de discuter des objectifs et du périmètre de l'audit de la protection de la vie privée, et de déterminer si la mission et la communication des constatations devraient être réalisées sous le sceau du secret professionnel liant l'avocat à son client.

5.1 Rôle de l'audit interne dans le dispositif de protection de la vie privée

Il incombe à la direction générale d'une organisation de décider du risque qu'elle est prête à prendre et de veiller à ce qu'existent les ressources nécessaires pour le gérer selon son appétence. Le traitement des risques d'atteinte à la vie privée englobe la mise en place d'un cadre de référence relatif à la protection de la vie privée approprié comprenant des politiques, des procédures et des contrôles. L'auditeur interne a pour rôle d'évaluer ce cadre, d'identifier les risques significatifs et de formuler les recommandations pertinentes pour le renforcer. L'évaluation du cadre de référence devrait prendre en compte les aspects suivants :

- La communication avec le conseiller juridique pour comprendre les conséquences juridiques :
  - La législation et la réglementation sur tous les territoires dans lesquels l'organisation opère.
  - L'impact de la législation et de la réglementation sur tous les territoires dans lesquels transitent, sont collectées ou stockées des données personnelles.
  - Déterminer si l'évaluation de la protection de la vie privée devrait être réalisée sous le sceau du secret professionnel.

- La communication avec les personnes responsables de la protection de la vie privée au sein de l'organisation afin de comprendre :
  - Les politiques et les directives internes concernant la protection de la vie privée.
  - Les politiques de protection de la vie privée établies à l'intention des clients et du public.
  - La qualité des contrôles de l'organisation dans le domaine de la protection de la vie privée.

- Les contacts avec les spécialistes des technologies de l'information et les gestionnaires de processus, afin d'y intégrer les éléments se rapportant à la sécurité de l'information :
  - Les politiques et procédures internes de sécurité.
  - Les politiques de sécurité communiquées aux clients et au public.
  - Les flux d'informations, les contrôles des systèmes, le stockage et l'utilisation des données personnelles.
  - Le plan de gestion des incidents.

Les domaines que l'audit interne peut revoir dans le cadre d'un audit de la protection de la vie privée comprennent généralement :

- La gouvernance / la supervision exercée par la direction.
- Les politiques de protection de la vie privée, et les contrôles y afférents.
- Les avertissements de confidentialité applicables.
- La nature, la pertinence des informations collectées.
- Les systèmes qui traitent, stockent et transmettent des données personnelles.
- Les méthodes de collecte.
- La gestion des inscriptions et des désinscriptions *(opt-in / opt-out)*.
- La conformité de l'utilisation de données personnelles en regard de l'objectif déclaré, la législation applicable et la réglementation.
- Les mesures de sécurité, les opérations et les contrôles techniques pour protéger les données personnelles.
- Les pratiques de conservation et de destruction des données personnelles.

De plus amples informations sont présentées dans l'Annexe « Matrice des faiblesses des contrôles de la protection de la vie privée et des actions à entreprendre – illustration ».

Les auditeurs internes devraient veiller à ne pas assumer la responsabilité de la conception et de la mise en œuvre du dispositif de protection de la vie privée, car cela pourrait compromettre leur indépendance. Compte tenu de la complexité de l'environnement réglementaire et technique affectant la protection de la vie privée, il convient de faire appel à un conseiller juridique et d'envisager de solliciter, le cas échéant, l'avis d'un expert externe.

5.2 Planification de la mission

Parmi les exemples de facteurs ayant trait à la protection de la vie privée susceptibles d'avoir un impact sur la nature des travaux de l'audit interne, citons :

- L'évolution constante de la législation et de la réglementation sur la protection de la vie privée des individus.
- La protection des données personnelles des individus dans le cadre d'accords avec des tiers / de *cloud computing*.
- La maturité des pratiques, politiques et procédures de l'organisation en matière de protection de la vie privée.
- Les nouvelles technologies et les stratégies commerciales qui exposent les données personnelles à un risque accru.
- L'externalisation et la délocalisation des processus qui collectent, utilisent, conservent, divulguent et détruisent les données personnelles.
- L'augmentation de la collecte, l'utilisation, la divulgation, la conservation et la destruction des données personnelles.
- Les risques constants d'atteinte à la vie privée qui soulignent la nécessité d'un plan global de gestion des incidents liés à la protection de la vie privée.

5.3 Hiérarchisation et classification des données

Un programme de recensement et de classification des données contribuera à identifier et à hiérarchiser les données critiques, dont les données personnelles nécessitant d'être protégées. L'auditeur devrait déterminer les niveaux de classification des données de l'organisation, le cadre utilisé pour classer les données, et les contrôles élémentaires mis en place pour chaque niveau de classification. À ce titre, l'auditeur peut se poser les questions suivantes :

- L'organisation dispose-t-elle d'une politique globale de classification des données ? Les niveaux de classification sont-ils appropriés pour permettre les contrôles adéquats ? Les catégories sont-elles convenablement définies ?
- Les données personnelles ont-elles été classifiées ?

Les niveaux de classification permettent-ils des contrôles adéquats de la protection de la vie privée ? La politique de classification des données personnelles a-t-elle été communiquée à ceux – y compris les prestataires de services externes – qui participent au traitement des données, de leur réception à leur destruction ? Existe-t-il un processus pour suivre les évolutions législatives et réglementaires qui auraient un impact sur la classification des données ? Les classifications sont-elles revues périodiquement afin de vérifier qu'elles restent appropriées ?

- La responsabilité de la détention et de la gestion des données personnelles a-t-elle été répartie au sein de l'organisation, et des contrôles appropriés ont-ils été mis en place en conséquence ?
- Quelles sont les sanctions légales et réglementaires applicables en cas de mauvaise gestion des données personnelles ? De quels recours juridiques disposent les individus qui s'en estiment victimes ?
- Quel préjudice un individu peut-il subir si les données ont été involontairement divulguées à des personnes non autorisées ?
- Dans quelle mesure une atteinte à la vie privée pourrait-elle être décelée et rapportée ?
- Qui en serait informé ? À travers quels circuits de communication ?
- Si des données personnelles étaient divulguées intempestivement, combien coûterait la réparation du préjudice ?
- À quelle hauteur une atteinte à la vie privée aurait-elle un impact sur la confiance des clients, des citoyens (dans le cas d'une entité publique) ou des investisseurs ? Quel serait le coût d'une restauration de cette confiance ?

5.4 Évaluation des risques

Lors de l'élaboration du programme d'audit, comme de la préparation de chaque mission, il convient de tenir compte de quatre grandes catégories de risques : risques juridiques et organisationnels, risques liés à l'infrastructure (technique), risques liés aux applications et aux processus opérationnels.

Risques juridiques et organisationnels

Les risques juridiques et organisationnels englobent les domaines tels que le non-respect de la législation et de la réglementation, l'absence de gouvernance et de direction concernant la protection de la vie privée, et l'insuffisance de ressources pour actualiser un programme efficace de protection de la vie privée. Dans le cadre de l'élaboration du plan d'audit de la protection de la vie privée, les questions devant être posées au titre des risques juridiques et pour l'organisation, comprennent :

- Qui sont les interlocuteurs désignés pour la protection de la vie privée ? Quel pourcentage de leur temps consacrent-ils à ces questions et est-ce adéquat ?
- Disposent-ils des connaissances, d'une autorité, d'un budget suffisant et du soutien de la direction générale pour mettre en œuvre et actualiser le dispositif de protection de la vie privée ?
- Comment les responsables de la protection de la vie privée actualisent-ils leur connaissance de la législation et la réglementation applicables à l'organisation ? Ont-ils identifié les obligations législatives et règlementaires relatives à la protection de la vie privée qui affectent les métiers ? Comment suivent-ils les évolutions législatives et réglementaires et évaluent-ils leur impact sur les politiques, les procédures et les systèmes de l'organisation ? Comment collaborent-ils avec les propriétaires des données pour mettre en œuvre les contrôles appropriés en réponse à ces évolutions ?
- En quoi les interlocuteurs concernés se sont-ils engagés dans l'évaluation des nouveaux projets opérationnels et des nouvelles technologies pour déterminer leur impact potentiel sur la protection de

la vie privée ?

- Si l'organisation utilise des services de *cloud computing,* les conséquences de la localisation des données et des éventuels transferts internationaux de données personnelles régis par des lois internationales sur la sécurité et sur la protection de la vie privée sont-elles prises en compte ? Les interlocuteurs gèrent-ils convenablement ces risques et ces exigences ?
- L'organisation a-t-elle prévu un plan de gestion des incidents liés à une atteinte à la vie privée ? Ce plan intègre-t-il les personnes adéquates ? Est-il documenté et à jour ? Comprend-il des conditions de notification d'atteinte à la vie privée en conformité avec les différentes réglementations internationales, nationales et locales ? Le plan de gestion d'atteintes à la vie privée comprend-il des étapes permettant de verrouiller les systèmes concernés afin de préserver les preuves nécessaires à une enquête ?
- Des modèles de documents nécessaires en réponse à une atteinte à la vie privée sont-ils déjà prêts, y compris un courrier de notification, les questions fréquemment posées par les victimes, les instructions aux clients concernant le gel des communications sur leurs avoirs et un communiqué de presse générique ?

Risques liés à l'infrastructure

Les objectifs de la sécurité de l'information consistent à assurer la confidentialité, l'intégrité et la disponibilité des données, rejoignant en cela ceux assignés à la protection de la vie privée. En conséquence, l'audit d'un dispositif de protection de la vie privée intègre obligatoirement un examen approfondi des contrôles relevant de la sécurité de l'information. Il peut être difficile de déterminer comment les informations à caractère personnel entrent et sortent de l'organisation, et où et comment les données circulent entre parties tierces à l'organisation.

Pour être utile, l'information doit entrer et sortir d'une application, tandis qu'elle change souvent de support pendant sa durée de vie. Elle peut ainsi, par exemple, commencer par se présenter sur du papier, être transportée via Internet, être traitée dans le *cloud*, obtenue de ou envoyée vers ou stockée sur des appareils mobiles, stockée sur un disque magnétique, imprimée et archivée dans une armoire, être sauvegardée sur un disque optique numérique pour être envoyée ultérieurement à l'extérieur à un tiers sur bande magnétique. À chaque fois que les données personnelles circulent et changent de format, de nouvelles vulnérabilités sont introduites.

Les broyeurs de papier, le chiffrement, les outils protégeant contre la fuite de données et bien d'autres pratiques empêchent la fuite de données sensibles. Les auditeurs internes devraient examiner le cycle de vie des données personnelles que l'organisation obtient, de la collecte à la destruction, et déterminer si elles sont gérées avec la diligence qui s'impose à chaque étape.

Les questions spécifiques à se poser lors de l'évaluation des risques liés à l'infrastructure qui menacent la protection de la vie privée sont notamment :

- L'organisation dispose-t-elle d'une cartographie des données à jour et d'un recensement de toutes les données personnelles, y compris leur localisation en interne ? Où les données circulent-elles au sein et en dehors de l'organisation ? Et comment sont-elles transférées entre les tiers impliqués dans le traitement des données personnelles pour le compte de l'organisation ? Chaque plateforme, base de données et autre élément de l'infrastructure technologique est associé à un risque propre qui doit être examiné.
- Les auditeurs internes devraient ainsi porter une attention particulière au parcours suivi par les données personnelles, que ce soit en transit vers les réseaux publics et privés, comme sur les supports envoyés par coursier. Ils doivent également suivre les

données stockées tout au long du processus de traitement, sans omettre le dispositif de sauvegarde et de reprise après sinistre. En particulier :
  - Comment les données personnelles sont-elles chiffrées lors de leur circulation au sein et en dehors de l'organisation et entre tiers ?
  - Les données personnelles stockées sur un média portable sont-elles chiffrées ?
  - Les données personnelles sont-elles stockées sous forme chiffrée ?
- Quel est le rôle des appareils mobiles dans la collecte, le traitement et le stockage des données personnelles dans l'organisation ?
- Quels contrôles généraux sont mis en place sur les plateformes des SI où les données personnelles sont traitées ou stockées, notamment les contrôles d'accès, la gestion des patchs et la recherche de vulnérabilités ?
- Les données personnelles sont-elles traitées ou stockées dans le *cloud* ? Les contrats de services de *cloud* comportent-ils des dispositions garantissant la sécurité de l'infrastructure et la mise en place de contrôles appropriés, et existe-t-il une clause de droit d'audit ?
- Si les données personnelles sont transférées ou copiées, après transfert, les données résiduelles sont-elles traitées avec les mêmes précautions que les données initiales ?

Risques liés aux applications

Déterminer, non seulement qui détient des informations sur votre compte, mais quelles sont ces informations, constitue un enjeu majeur en matière d'identification des risques d'atteinte à la vie privée. Les logiciels apportent vitesse d'exécution et exactitude à de nombreuses fonctions manuelles sujettes à erreur. Malheureusement, les systèmes logiciels sont aussi complexes, et peuvent donc conduire à des failles et des comportements imprévus. Il n'est pas simple d'évaluer les fonctions des systèmes destinés à traiter, mettre en commun et diffuser leurs données. En effet ces systèmes combinent souvent une mise en œuvre de logiciels développés en interne, avec des logiciels achetés dans le commerce, des applications basées sur le *cloud* et, le cas échéant modifiés pour les adapter au contexte local, auxquels s'ajoutent les fonctions spécifiques des systèmes d'exploitation et des interlogiciels *(middleware)* pour traiter, partager et distribuer les données.

Une fois que l'auditeur a identifié les processus automatisés gérant des données personnelles, des questions extrêmement importantes se posent concernant la sécurité des applications correspondantes :

- Une évaluation des risques liés à la protection de la vie privée a-t-elle été réalisée afin d'identifier et de traiter les problématiques relatives à la protection de la vie privée au cours du développement du logiciel ? L'une des méthodes de « protection de la vie privée dès la conception » intègre une sensibilisation à la protection de la vie privée à chacun des aspects des activités quotidiennes, y compris au développement d'applications et de processus nouveaux impliqués dans la collecte et l'utilisation de données personnelles.
- Des normes de classification des données ont-elles été appliquées lors de la conception de l'application, afin de mettre en place des contrôles de base appropriés pour la protection des données personnelles et des informations traitées par celle-ci ?
- Dans quelle mesure la conformité du développement et du déploiement de l'application et les contrôles associés ont-ils été vérifiés par rapport aux spécifications fonctionnelles prescrites ?
- Comment l'application gère-t-elle l'authentification et l'accréditation des utilisateurs autorisés ? Quels sont les profils utilisateurs prévus dans l'application pour limiter l'accès au « minimum nécessaire » selon les responsabilités concernées ? Les autorisations sont-elles raisonnables ?
- Existe-t-il des pistes d'audit traçant l'accès des utili-

sateurs aux données afin de s'assurer que toutes les tentatives d'accès qui ont échoué ou réussi peuvent faire l'objet de recherches et qu'une responsabilité puisse être attribuée ?

- Existe-t-il des interfaces externes vers d'autres applications ? Ces applications exercent-elles un contrôle de niveau équivalent concernant la protection des données personnelles ?
- Quel est le processus pour la maintenance des applications ainsi que des bases de données auxquelles celles-ci accèdent ?
- Qui répond aux problèmes de sécurité potentiels et veille à ce que les patchs de sécurité soient testés et appliqués ?
- Qui est responsable de la sécurité générale de l'application ?
- Lors du développement et des tests des applications, utilise-t-on des jeux d'essais ou les données de production personnelles ou sensibles ont-elles été correctement rendues anonymes ? Si tel n'est pas le cas, les contrôles dans l'environnement de test sont-ils équivalents à ceux mis en œuvre dans l'environnement de production ?
- L'application prévoit-elle le traitement ou le stockage des données personnelles dans le *cloud* ? Le cas échéant, les contrôles sont-ils équivalents aux contrôles requis pour les applications internes traitant les données personnelles ?
- Quels types de cookies, de balises Internet ou de pixels Internet sont utilisés pour les applications Internet de l'organisation ? Sont-ils destinés à un usage interne ou pour collecter des informations pour des tiers ? Quel type de données personnelles sont collectées, comment sont-elles utilisées et, si elles sont sensibles, comment l'accord de l'utilisateur est-il obtenu et stocké ? Veiller à l'utilisation transparente de ces technologies de suivi et de collecte des informations constitue un point clé des litiges et des réglementations actuels sur la protection de la vie privée.
- Existe-t-il des applications effectuant une géolocalisation afin de fournir des services ou d'obtenir des données personnelles de la part des clients ? Le cas échéant, quelles données personnelles sont collectées, comment sont-elles utilisées et, si elles sont sensibles, comment l'accord de l'utilisateur est-il obtenu et stocké ?

Risques liés aux processus opérationnels

Au-delà des efforts déployés par les informaticiens pour protéger, chiffrer et de façon générale sécuriser les données personnelles, le traitement de ces dernières exige que leur utilisation soit conforme aux fins prévues. Il importe en conséquence que chaque intervenant dans le traitement de données personnelles respecte leur degré de sensibilité (classification). La protection des informations imprimées doit suivre également les mêmes principes que ceux appliqués à la classification et à la protection des données électroniques. C'est ainsi que les bureaux devraient, au minimum, être « nets » de documents et les armoires et meubles d'archivage verrouillés, et la destruction des documents devrait être sécurisée. Dans les zones ouvertes au public, des principes de discrétion doivent être institués et appliqués. Les évaluations des risques, les procédures de traitement et les programmes de formation et de sensibilisation devraient contribuer à identifier et à minimiser les risques d'atteinte à la vie privée dans les processus.

5.5 Préparation de la mission

La MPA 2130.A1-2 couvre les activités d'audit interne se rapportant au cadre de protection de la vie privée d'une organisation. Ces activités consistent à :

- Évaluer le caractère adéquat de l'identification par la direction des risques liés à ses objectifs en matière de protection de la vie privée.
- Évaluer le caractère adéquat des contrôles mis en place pour limiter les risques d'atteinte à la vie privée.

- Identifier la nature et la pertinence des données personnelles collectées, ainsi que la méthode de collecte, et déterminer si l'usage que fait l'organisation de ces informations correspond à celui prévu et à la législation applicable.
- Donner une assurance concernant l'efficacité des politiques, des pratiques et des contrôles de l'organisation en matière de protection de la vie privée.

Plusieurs ouvrages et réglementations fournissent une approche pour mettre en place et réaliser des audits de dispositifs de protection de la vie privée. C'est ainsi que le *Privacy Handbook*[4], lui-même reprenant les critères de l'OCDE propose un modèle intuitif pour bâtir un plan d'audit. L'ouvrage *Privacy – Assessing the Risk*[5] présente quant à lui un plan d'audit plus exhaustif et davantage orienté sur la technologie. Le référentiel *Generally Accepted Privacy Principles – A Global Privacy Framework* de l'AICPA / CICA, qui contient des principes, des concepts clés et les principales législations et réglementations internationales relatives à la protection de la vie privée peut être très utile lors de l'élaboration de thèmes sur la protection de la vie privée à inclure dans le programme d'audit, comme indiqué dans la Figure 4.

Évaluations de la protection de la vie privée

De nombreuses instances législatives et réglementaires imposent, ou au minimum recommandent, des évaluations de la protection de la vie privée. Nombre d'organisations comprennent également qu'un dispositif de contrôle interne, opérationnel et piloté par les risques, doit intégrer l'évaluation de la pertinence et de l'efficacité de leurs politiques et pratiques en matière de protection de la vie privée. Les modèles d'évaluation existants fournissent des recommandations détaillées pour la mise en place de missions d'audit.
Il convient tout d'abord de définir les objectifs d'une évaluation du dispositif de la protection de la vie privée, par exemple :

- Déterminer les risques inhérents et résiduels.
- Apporter une assurance sur la qualité des contrôles limitant les risques d'atteinte à la vie privée.
- Vérifier l'adhésion à un ensemble de normes et de réglementations y afférent.
- Veiller à la conformité des instructions internes en matière d'utilisation, de collecte, de conservation, de protection et de destruction des données personnelles.

Le manuel d'audit sur la protection des données du commissaire à l'information au Royaume-Uni *(U.K Information Commissioner's Data Protection Audit Manual)* décrit une méthode pour effectuer des missions de conformité de la protection des données et présente des listes de tests de conformité au Data Protection Act de 1998 (loi britannique sur la protection des données). Ce manuel d'audit est conçu pour permettre à tout contrôleur ou propriétaire de données de juger de la conformité de son organisation en matière de protection des données. Il peut également être utilisé par n'importe quelle organisation offrant de tels services à des contrôleurs de données. Le manuel décrit les processus généraux d'audit de dispositifs de protection de la vie privée : à titre externe ou interne, leur pertinence et leur conformité, et selon une approche verticale (fonctions) ou horizontale (processus). Les auditeurs internes peuvent commencer par délimiter le périmètre à auditer : l'ensemble de l'organisation, une fonction, un processus ou une catégorie d'informations. Un audit exhaustif couvre tous les aspects de protection de la vie privée. Une approche par les risques se fonde sur leur impact et leur probabilité d'occurrence et privilégie l'analyse des domaines les plus exposés, exprimés en termes de structures, de processus et de nature de données.

[4] Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues / Albert J. Marcella Jr.,Carol Stucki . - John Wiley & Sons, 23 mai 2003.
[5] Privacy: Assessing the Risk / Kim Hargraves. - Institute of Internal Auditors Research Foundation, 2003.

Il existe des programmes de travail prêts à l'emploi élaborés par les organes de supervision, les associations sectorielles et les défenseurs de la vie privée, qui indiquent les travaux d'audit obligatoires et constituent un bon point de départ pour des audits ponctuels, ou récurrents, mais customisés. Le responsable de l'audit interne, ou son délégué, devrait examiner ou valider tout programme de travail avant le début d'une mission visant la protection de la vie privée. Lorsqu'un commissaire à la protection de la vie privée, ou une fonction analogue, commande ou exécute des revues de la protection des données personnelles, les auditeurs internes devraient analyser le caractère suffisant de ces évaluations et l'efficacité de leur suivi.

Préalables à une mission d'audit de la protection de la vie privée – compréhension des données

Il importe de comprendre que la conformité à la législation et à la réglementation en vigueur est fondamentale et devrait faire partie intégrante d'une évaluation exhaustive des risques d'atteinte à la vie privée et d'un audit dans une organisation. De plus, lorsqu'ils planifient une mission visant la protection de la vie privée, les auditeurs internes devront :

- Avoir une vision d'ensemble des données personnelles collectées et stockées, de leur utilisation par l'organisation, de leur traitement par la technologie et des juridictions / pays dans lesquels les données sont traitées.
- Interroger les personnes responsables de la politique de protection de la vie privée et de sa mise en œuvre et/ou des juristes en interne ou en externe, afin de mieux comprendre la législation et la réglementation régissant l'activité et le type d'informations gérées, ainsi que les risques identifiés, les contrôles prescrits et les incidents rencontrés.
- Identifier la législation et la réglementation régissant les données personnelles dans les juridictions où l'organisation opère.
- Déterminer quelles sont les autorités publiques et la réglementation susceptibles d'encadrer l'application des règles de protection de la vie privée. Demander au correspondant Informatique et liberté ou à la personne chargée de la protection de la vie privée la manière dont cette réglementation a été intégrée à la politique et aux procédures internes.
- Déterminer quelles sont les données personnelles des clients, des salariés et des partenaires que l'organisation collecte et qui doivent faire l'objet d'une protection. Si un recensement des données existe, il peut constituer un point de départ pour l'auditeur. En l'absence de recensement documenté, il peut être nécessaire d'interroger les propriétaires des processus et leurs interlocuteurs chargés des SI afin de déterminer les données personnelles collectées. Les outils de détection automatique peuvent également aider l'auditeur interne durant cette étape.
- Identifier les données personnelles qui sont, le cas échéant, partagées avec des tiers. Déterminer comment ces données sont communiquées à chacun de ces tiers, y compris les copies papier, les transferts de fichiers et les médias électroniques portables. L'idée est d'identifier les moyens formels et informels à travers lesquels les données personnelles sont partagées au sein de l'organisation et avec d'autres entités, afin de repérer les menaces, les vulnérabilités et le risque global. Déterminer si des accords avec des prestataires et des partenaires externes prévoient des contrôles appropriés pour le traitement des données personnelles de leur réception à leur destruction.

Identifier les menaces liées à la protection de la vie privée

Les auditeurs internes devraient repérer les menaces qui pèsent sur les données de l'organisation au moyen de recherches, études comparatives et réflexions innovantes, afin de classer celles-ci selon leur probabilité

d'occurrence et leur impact. Les ateliers d'évaluation des risques avec les propriétaires des processus permettent également de s'assurer que les risques et les menaces sont analysés et identifiés de façon approfondie. L'évaluation des menaces et des actifs au regard du risque d'atteinte à la vie privée permet de déterminer les points majeurs où doivent se concentrer les contrôles et les dispositifs de maîtrise, de même ceux sur lesquels les auditeurs devraient se focaliser pour détecter les vulnérabilités.

Une menace utilise une vulnérabilité pour exploiter un actif. En matière de protection de la vie privée, l'actif est constitué par les données personnelles protégées. Quelle est la nature de la menace ou d'où provient-elle ? La menace est un indicateur sur le processus qui, volontairement ou non, rend publiques les données à caractère personnel d'une organisation ou permet un accès non autorisé à des données à caractère personnel. Une menace légitime peut être la violation, par un partenaire externe, de ses engagements contractuels, ou un pirate informatique à la solde du crime organisé. L'expérience démontre que les salariés, le personnel contractuel, ou en mission temporaire, les concurrents, les développeurs, les concierges ou les agents de maintenance, tous ceux qui disposent d'un accès autorisé aux lieux où les données confidentielles sont stockées, représentent des menaces. Que ce soit par malveillance ou par négligence, ces individus ayant accès aux données personnelles ont la possibilité de les divulguer. En cas de partage de données protégées avec des tiers (partenaires, fournisseurs…), il convient d'évaluer spécifiquement les menaces supplémentaires induites.

Identifier les contrôles et les dispositifs de maîtrise

Afin de déterminer ce que l'organisation fait pour protéger les données personnelles des menaces les plus importantes, les auditeurs internes devraient valider l'infrastructure et les contrôles généraux existants, ainsi que les dispositifs de maîtrise, qui sont actifs et utilisés dans le cadre de la protection de la vie privée. Voici les étapes habituelles d'une identification de ces contrôles :

- **Demander et passer en revue la documentation.** Examiner la démarche de protection de la vie privée telle que celle-ci est mise en œuvre à travers les politiques, procédures et d'autres documents. Comment les politiques en place recouvrent-elles les domaines à haut risque mis en évidence dans l'évaluation des risques d'atteinte à la vie privée? Le cas échéant, à quelle fréquence ces politiques sont-elles révisées ? Incorporent-elles les dernières recommandations en date édictées par la législation et la réglementation ? Les recommandations sont-elles homogènes pour toutes les divisions de l'organisation ? Existe-t-il d'éventuels écarts à surveiller ultérieurement ?

- **Mener des interviews et observer le traitement des données personnelles sur le terrain.** L'écart entre la politique formulée par écrit et l'action sur le terrain peut être important. Rapprochez-vous des opérationnels et de la direction des systèmes d'information et déterminez s'ils sont conscients de l'impact de leurs actions / processus en matière de gestion des données personnelles. Déterminez également si des contrôles non documentés existent, et si l'esprit comme la lettre du dispositif de protection de la vie privée motivent les décisions et les actes du personnel.

- **Examiner les contrats et les contacts avec les tiers.** La profondeur de l'examen dépend de la place qu'occupent les prestataires et leur gestion des données dans la matrice des menaces. Au minimum, l'auditeur interne devrait examiner si la terminologie utilisée est conforme à la législation et à la réglementation applicables. Si des clauses d'audit sont incluses, sont-elles exercées avec la fréquence et la profondeur requises ? Les enquêtes ou les ques-

tionnaires sur la sécurité / les contrôles de la protection de la vie privée représentent une autre technique courante pouvant être utilisée par les auditeurs lors de l'examen des tiers. L'auditeur peut ainsi obtenir des informations sur les contrôles mis en place par le tiers pour protéger les données personnelles de l'organisation, et identifier des domaines pouvant nécessiter un suivi.

Une défaillance des contrôles ou une faiblesse dans la conception, le fonctionnement ou l'efficacité des contrôles des tiers, peuvent porter atteinte à la confidentialité et à la protection des données personnelles. Dès lors, les contrats passés avec les prestataires externes constituent un élément critique et devraient contenir des dispositions relatives à la protection de la vie privée, et assurer la confidentialité des données et des applications.

À ce stade, un recentrage sur les risques potentiels à fort impact sera envisageable. C'est le moment de tester les contrôles et les dispositifs de maîtrise, de classer les actifs en fonction de leur impact et de modéliser les menaces représentant l'impact le plus fort.

5.6 Évaluation

Les étapes courantes d'une mission d'audit sont décrites dans le *Cadre de Référence International des Pratiques Professionnelles de l'audit interne* (CRIPP) de l'IIA *(International Professional Practices Framework)*. Une fois que l'auditeur a compris les objectifs de l'organisation, les risques auxquels elle est confrontée, les catégories de données personnelles gérées et le cadre juridique dans lequel l'organisation opère, il convient d'élaborer et de faire valider un programme d'audit précisant le périmètre, les objectifs et le calendrier de la mission. L'équipe d'audit collecte ensuite les informations, effectue des tests et en analyse les résultats afin de rédiger son rapport et ses recommandations.

Méthodes de test

Une fois l'évaluation des risques achevée, les tests classiques portent sur les contrôles généraux applicatifs et de sécurité. Les tests peuvent également être plus spécifiques et consister en des évaluations de vulnérabilités, des tests d'intrusion, ou bien encore des contrôles physiques ou ceux recourant à l'ingénierie sociale.

Évaluation des vulnérabilités et tests d'intrusion

Ces méthodes sont souvent considérées comme des méthodes d'évaluation spécifiques aux applications et aux systèmes accessibles à travers un réseau. Les consultants utilisent souvent des termes tels que *« tiger team »* (équipe « de choc ») ou *« ethical hacking »* (piraterie éthique) pour décrire cette méthode de détection et d'exploitation des vulnérabilités dans un environnement de production.

L'évaluation des vulnérabilités s'attache en général à les identifier et à les classer par ordre de priorité en fonction de la configuration des systèmes d'information, de leur administration et de leur architecture. Les tests d'intrusion renforcent ces évaluations, car ils exploitent des vulnérabilités révélées. Ces tests requièrent en général des compétences techniques plus pointues et sont susceptibles de perturber le fonctionnement des systèmes de production. L'évaluation des vulnérabilités et les tests d'intrusion nécessitent un ensemble de compétences que l'auditeur interne devra acquérir, soit en sollicitant un expert extérieur, soit en se formant.

Tests des contrôles physiques

Les données personnelles numériques ne sont pas les seules informations à caractère personnel. Si la menace a accès au bâtiment, aucun chiffrement, pare-feu ou patch de base de données au monde ne pourra empêcher un individu de récupérer des informations impri-

mées dans les poubelles, ou d'accéder aux données depuis un poste de travail non verrouillé. Fouiller les poubelles pour y trouver des informations protégées, repérer les postes provisoirement abandonnés par leur utilisateur avec une session de travail ouverte, et passer en revue le stockage sécurisé de l'information ainsi que les procédures de traitement, permet de détecter les vulnérabilités dans la gestion des données personnelles. Ce type de test peut répondre à des questions telles que :

- La destruction des données personnelles s'effectue-t-elle conformément aux politiques et procédures en vigueur ?
- Les documents contenant des données personnelles sont-ils conservés de manière sécurisée, avant d'être détruits ou passés à la broyeuse ?
- Les documents de travail contenant des données personnelles sont-ils conservés de manière sécurisée ?
- Du personnel non autorisé est-il susceptible d'accéder à des documents ou aux écrans qui affichent des informations confidentielles ?
- Les postes de travail sont-ils verrouillés lorsque leurs titulaires sont absents ?
- La mise en œuvre des contrôles de protection de la vie privée est-elle homogène d'un service à l'autre ?

Tests d'ingénierie sociale

Dans le contexte de la sécurité, l'ingénierie sociale est une technique qui consiste à obtenir un accès non autorisé en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes, sans recourir à des moyens techniques. Dans le cadre d'un test portant sur le dispositif de protection de la vie privée, il est possible de recourir à l'ingénierie sociale pour tester l'efficacité des contrôles concernant la diffusion de données personnelles. Cela permet de savoir quelles données personnelles un individu peut obtenir simplement en les demandant. L'auditeur interne peut se faire passer pour un dirigeant, un administrateur de réseau ou tout autre utilisateur autorisé pour obtenir des mots de passe ou des données personnelles, par duperie ou à la faveur de conversations « anodines » avec des salariés qui sont des acteurs clés des dispositifs de maîtrise. Les tests d'ingénierie sociale permettent de répondre aux questions suivantes :

- Quelle est l'efficacité des programmes de sensibilisation et de formation à la protection de la vie privée mis en place par l'organisation ?
- Existe-t-il un équilibre approprié entre service à la clientèle et restriction de l'accès à l'information ?
- Le dispositif de protection de la vie privée peut-il s'appuyer sur la culture d'entreprise ?

Les organisations peuvent avoir des réactions différentes vis-à-vis du recours, par les auditeurs internes, à une duperie volontaire de leurs salariés. Il convient donc d'être très prudent dans la mise en œuvre d'une telle démarche pour modéliser les menaces et mettre en lumière les vulnérabilités. Il est indispensable d'en discuter avec les services juridique et ressources humaines, et veiller ensuite à ce que les résultats obtenus soient utilisés pour améliorer le dispositif de protection de la vie privée, et non pour constituer une cause de licenciement à l'encontre des salariés ayant été visés par le test.

5.7 Communication et suivi des résultats

Nombre de missions d'audit interne portant sur la protection de la vie privée sont des évaluations visant la conformité. L'auditeur devrait consulter le conseiller juridique si des violations potentielles doivent être incluses dans le rapport d'audit. La consultation de ce conseiller et sa participation à la coordination des travaux peuvent ainsi atténuer des conflits potentiels entre les responsabilités de l'auditeur interne, qui doit consigner par écrit les résultats de sa mission, et l'obligation faite au conseiller juridique de défendre l'organisation.
Voici certaines des précautions à prendre lors de la communication des résultats d'une mission d'audit

interne relative à la protection de la vie privée :

- Obtenir la participation de tous ceux qui sont dans le périmètre de l'audit de la protection de la vie privée. Pour être efficace, un dispositif de protection de la vie privée doit être appliqué dans pratiquement toutes les parties d'une organisation. Il faut veiller à ce que tous les participants clés y contribuent.
- Élaborer un langage commun compréhensible pour décrire les risques.
- Veiller à ce que le conseiller juridique ait examiné le programme de travail proposé et le projet de rapport avant sa diffusion, pour être certain que les questions de conformité sont traitées correctement.

Le RAI devrait connaître la Norme de fonctionnement 2600 « Communication relative à l'acceptation des risques », au cas où il estimerait que la direction générale a accepté un niveau de risque résiduel pouvant être inacceptable compte tenu du dispositif et des pratiques de protection de la vie privée de l'organisation.

5.8 Protection de la vie privée et gestion des audits

Le CRIPP rappelle aux auditeurs de tenir compte des risques et de la réglementation sur la protection de la vie privée lorsqu'ils planifient, exécutent et rendent compte de leurs missions d'assurance et de conseil. Bon nombre d'organisations professionnelles, de législateurs et d'organes de supervision publient un large éventail de recommandations et de règles. La confidentialité des données personnelles et la façon dont l'organisation gère cet actif devraient être prises en compte lors de l'élaboration du plan d'audit fondé sur les risques.

Les auditeurs internes constituent un élément clé de la structure de gouvernance de l'organisation en matière de protection de la vie privée. Aussi, des programmes et des politiques de formation devraient être mis en place afin de procurer aux auditeurs internes la culture, les connaissances nécessaires à une réalisation efficace des missions relatives à la protection de la vie privée. Il convient également de vérifier que les auditeurs internes respectent la législation et la politique en vigueur lorsqu'ils utilisent des données personnelles pendant des missions d'assurance ou de conseil. Les auditeurs internes devraient comprendre que, dans certains cas, il peut être illégitime, voire illégal, de consulter, récupérer, examiner, manipuler ou utiliser des données personnelles au cours d'une mission d'audit interne. Avant d'entamer une mission, les auditeurs internes devraient se renseigner sur ces problématiques et, le cas échéant, demander l'avis du conseiller juridique interne. En outre, les auditeurs internes devraient tenir compte des prescriptions législatives et réglementaires se rapportant à la protection de la vie privée lorsqu'ils communiquent des informations à l'extérieur de l'organisation.

VI. 12 QUESTIONS QUE LE RESPONSABLE DE L'AUDIT INTERNE DEVRAIT SE POSER CONCERNANT LA PROTECTION DE LA VIE PRIVÉE

1. L'organisation a-t-elle mis en place un organe de gouvernance pour décider du niveau de risque qu'elle accepte de prendre en matière de protection de la vie privée ?

2. Quel niveau de risque le management est-il prêt à accepter dans le domaine de la protection de la vie privée ?

3. À quelles législations et réglementations l'organisation est-elle actuellement soumise en matière de protection de la vie privée et lesquelles sont susceptibles d'être applicables à l'avenir ?

4. Quelles sont les données personnelles que l'organisation collecte ? Qui définit ce que sont des données personnelles et des informations confidentielles ? Ces définitions sont-elles cohérentes et appropriées ?

5. L'organisation s'est-elle dotée de politiques et de procédures pour la collecte, l'utilisation, la conservation, la destruction et la divulgation des données personnelles ?

6. L'organisation a-t-elle désigné un responsable pour la gestion de son dispositif de protection de la vie privée ?

7. L'organisation sait-elle où sont stockées toutes les données personnelles et qui y a accès ?

8. Comment sont protégées les données personnelles à différents niveaux - bases de données, réseaux, plateformes système, couches d'application et processus / fonctions ?

9. Parmi les données personnelles collectées par l'organisation, certaines sont-elles divulguées à ou traitées par des tiers ?

10. Les salariés suivent-ils une formation sur la sensibilisation aux données personnelles, et reçoivent-ils des orientations concernant leurs responsabilités pour la gestion des obligations, problèmes et autres problématiques de protection de la vie privée ?

11. L'organisation dispose-t-elle et fournit-elle des ressources adéquates pour élaborer, mettre en œuvre et actualiser un dispositif efficace de protection de la vie privée ?

12. L'organisation procède-t-elle à une évaluation périodique de la mise en application de ces politiques et procédures de protection de la vie privée tout en vérifiant que les obligations actuelles ou nouvelles sont respectées ?

VII. ANNEXE

Le Cadre de Référence International des Pratiques Professionnelles de l'audit interne (CRIPP) de l'IIA

Les lignes directrices officielles d'audit interne sont énoncées dans le CRIPP, qui comprend des dispositions obligatoires et des dispositions recommandées. Les trois dispositions obligatoires du CRIPP sont la définition de l'audit interne, le Code de déontologie et les Normes Internationales pour la Pratique Professionnelles de l'audit interne (Normes). Les trois dispositions recommandées du CRIPP sont les prises de position, les modalités pratiques d'application (MPA) et les guides pratiques.

Des lignes directrices spécifiques peuvent être consultées dans le Code de déontologie, les Normes et les MPA de l'IIA. Des parties importantes de ces lignes directrices sont exposées ci-après.

Code de déontologie

La section sur la confidentialité précise que les auditeurs internes :

- Doivent utiliser avec prudence et protéger les informations recueillies dans le cadre de leurs activités.
- Ne doivent pas utiliser ces informations pour en retirer un bénéfice personnel, ou d'une manière qui contreviendrait aux dispositions légales ou porterait préjudice aux objectifs éthiques et légitimes de leur organisation.

Modalités pratiques d'application (MPA)

Bien que dans certains cas, les MPA suivantes ne portent pas directement sur la protection de la vie privée, ce sont des MPA clés que l'auditeur interne devrait connaître pour évaluer le dispositif de protection de la vie privée d'une organisation :

2010-1 : Prise en compte des risques et des menaces pour l'élaboration du plan d'audit
2010-2 : Prise en compte du management des risques dans la planification de l'audit interne
2120-1 : Évaluer la pertinence des processus de management des risques
2120-2 : Gestion du risque lié à l'activité d'audit interne
2130-1 : Évaluer la pertinence des processus de contrôle
2130-A1-2 : Evaluation du dispositif mis en place par l'organisation pour protéger la vie privée
2200-2 : Utilisation d'une approche « Top-Down », fondée sur les risques, pour identifier les contrôles à évaluer dans le cadre d'une mission d'audit interne
2300-1 : Utilisation d'informations à caractère personnel dans la conduite d'une mission

Matrice des faiblesses des contrôles de la protection de la vie privée et des actions à entreprendre - illustration

Des exemples de faiblesses éventuelles des contrôles de la protection de la vie privée et d'actions pouvant être entreprises par l'auditeur interne pour y remédier sont présentés ci-après. Ces exemples ne sont pas censés être exhaustifs et peuvent ne pas s'appliquer à votre environnement.

FAIBLESSES DES CONTROLES	ACTIONS
L'organisation n'a pas mis en place de politique relative à la protection de la vie privée, ni de dispositif de contrôle approprié.	Discuter avec la direction générale de la nécessité d'une politique bien documentée relative à la protection de la vie privée et de l'élaboration d'un dispositif efficace dans ce domaine.
L'organisation ne se conforme pas à sa politique de protection de la vie privée.	Mener une revue de ses pratiques et comportements pour s'assurer que l'organisation respecte les engagements qu'elle a pris envers ses clients dans sa déclaration relative à la protection de la vie privée.
L'organisation ne protège pas correctement les données personnelles qu'elle collecte, utilise, conserve, divulgue et détruit.	Mener une revue de la sécurité de l'information (contrôles administratifs, physiques et techniques) pour s'assurer que l'organisation protège correctement les données personnelles.
L'organisation n'a pas défini les catégories de données personnelles qu'elle collecte, ni qui y a accès, ni où ces données sont stockées.	Identifier les flux de données qui, dans le système, correspondent aux données personnelles collectées, les personnes qui y ont accès et les besoins de l'entreprise en la matière.
L'organisation n'a pas documenté l'objectif de la collecte de données personnelles afin d'assurer qu'elle ne collecte et ne conserve pas plus de données que nécessaire.	Cartographier les flux de données personnelles collectées au travers des systèmes automatisés ou des processus manuels et identifier l'objectif de la collecte et de la conservation.
L'organisation ne dispose pas d'une structure de gouvernance formelle en ce qui concerne le respect des principes de protection de la vie privée.	Discuter avec la direction générale, et le cas échéant avec le Conseil, de l'opportunité de mettre en place une structure de gouvernance pour faire respecter les principes de protection de la vie privée.
L'organisation n'a pas de politique interne qui renforce la protection des données personnelles.	Mener une revue des politiques, ses normes et ses procédures relatives à la protection des données personnelles pour s'assurer qu'elles couvrent des aspects tels que la classification des données, la gestion des fichiers, la conservation et la destruction des données.
L'organisation n'a pas établi de référentiel de contrôle permanent d'audit de la conformité.	Inclure la protection de la vie privée dans le recensement des cibles d'audit fondé sur une approche par les risques. Demander au service juridique un inventaire de la législation et de la réglementation applicables à l'organisation. Mener un audit portant spécifiquement sur la protection de la vie privée.
L'organisation n'a pas mis en place de plan de gestion des incidents.	Discuter avec la direction générale, y compris avec la direction informatique et le service juridique, de la nécessité de mettre en place un plan de gestion des incidents en cas d'infraction aux principes de protection des données personnelles.

FAIBLESSES DES CONTROLES	ACTIONS
L'organisation ne propose pas de programme de formation sensibilisant à la protection de la vie privée, à la gestion des données ou à la sécurité de l'information.	Mener une revue des moyens de formation et de sensibilisation mis en œuvre concernant la protection de la vie privée, afin de déterminer s'ils répondent aux besoins de l'organisation. Analyser les dossiers de formation pour s'assurer que le personnel qui gère ou qui a accès à des données personnelles a reçu une formation appropriée.
N'appliquant pas de programme de gestion de la sécurité et de protection de la vie privée vis-à-vis de ses prestataires extérieurs, l'organisation ne dispose pas d'une approche homogène de la sous-traitance, de l'évaluation et du pilotage des pratiques de ses fournisseurs en matière de protection de la vie privée.	Mener une revue des contrats signés avec les prestataires pour s'assurer qu'ils contiennent les éléments clés nécessaires à la protection des données personnelles, notamment en matière de résiliation, les clauses de destruction des fichiers contenant des données personnelles ainsi qu'une clause d'audit. Réaliser des missions périodiques permettant de s'assurer que les prestataires se conforment aux dispositions du contrat.

Auteurs :
Ken Askelson, CIA, CPA, CITP, CGMA
Stefanie Hardgrove, CIA, CPA, CIPP/IT
Michael Lynn, CPA
Sara Lademan, CIA, CISA, CGEIT, CISSP
David Williams, CISA, PCI-ISA

Réviseurs :
Steve Hunt, CIA, CBM, CGEIT, CISA, CRISC, CRMA
Steven Jameson, CIA, CBA, CCSA, CFE, CFSA, CGMA, CPA, CRMA

Relecteurs :
Marie-Elisabeth Albert, CIA
Christophe Butikofer, CIA
Julien Cornuché, CIA
Béatrice Ki-Zerbo, CIA
Yann Le Bourthe
Jacques Renard

A PROPOS DE L'INSTITUTE OF INTERNAL AUDITORS

Fondé en 1941, The Institute of Internal Auditors (IIA) est une organisation professionnelle internationale dont le siège mondial se situe à Altamonte Springs, en Floride, aux États-Unis. L'Institute of Internal Auditors est la voix mondiale, une autorité reconnue, un leader incontesté et le principal défenseur de la profession d'auditeur interne. C'est également un acteur de premier plan pour la formation des auditeurs internes. Il est représenté en France par l'IFACI.

A PROPOS DES GUIDES PRATIQUES

Les guides pratiques détaillent la réalisation des activités d'audit interne. Ils contiennent des processus et des procédures, tels que les outils et techniques, les programmes et les approches pas-à-pas, et donnent des exemples de livrables. Les guides pratiques s'inscrivent dans le Cadre de référence international des pratiques professionnelles de l'audit interne de l'Institute of Internal Auditors. Ces guides pratiques relèvent de la catégorie des dispositions fortement recommandées. La conformité à ces guides pratiques n'est donc pas obligatoire, mais fortement recommandée. Ces guides ont été officiellement révisés et approuvés par l'IIA.

Pour de plus amples informations sur les documents de référence proposés par l'Institute, vous pouvez consulter notre site Web, www.theiia.org.guidance ou www.ifaci.com.

AVERTISSEMENT

L'Institute of Internal Auditors publie ce document à titre informatif et pédagogique. Cette ligne directrice n'a pas vocation à apporter de réponses définitives à des cas précis, et doit uniquement servir de guide. L'Institute of Internal Auditors vous recommande de toujours solliciter un expert indépendant pour avoir un avis dans chaque situation. L'Institute dégage sa responsabilité pour les cas où des lecteurs se fieraient exclusivement à ce guide.

COPYRIGHT

Le copyright de ce guide pratique est détenu par l'Institute of Internal Auditors et par l'IFACI pour sa version française. Pour l'autorisation de reproduction, prière de contacter l'Institute of Internal Auditors à l'adresse guidance@theiia.org ou l'IFACI à l'adresse recherche@ifaci.com

The Institute of Internal Auditors
247 Maitland Avenue, Altamonte Springs, Florida 32701, États-Unis
Téléphone : +1 407 937 1100
Télécopie : 1 407 937 1101
Site Web : www.theiia.org
Courrier électronique : guidance@theiia.org

IFACI
98bis, Bulevard Haussmann
75008 PARIS, France
Téléphone : 01 40 08 48 00
Fax : 01 40 08 48 20