NORME INTERNATIONALE

ISO/IEC 29134

Première édition
2017-06

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'étude d'impacts sur la vie privée

Information technology — Security techniques — Guidelines for privacy impact assessment

Numéro de référence
ISO/IEC 29134:2017(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organismes internationaux, gouvernementaux et non gouvernementaux, en liaison avec l'ISO et l'IEC participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/avant-propos.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Introduction

Une évaluation des impacts sur la vie privée (PIA) est un instrument permettant d'évaluer les impacts potentiels sur la vie privée d'un processus, d'un système d'information, d'un programme, d'un module logiciel, d'un dispositif ou de toute autre initiative qui traite des données à caractère personnel (DCP) et, en consultation avec les parties prenantes, de prendre les mesures nécessaires afin de gérer les risques sur la vie privée. Un rapport PIA peut comprendre une documentation concernant les mesures adoptées pour traiter les risques, par exemple les mesures découlant de l'utilisation du système de management de la sécurité de l'information (SMSI) comme décrit dans l'ISO/IEC 27001. Un PIA ne se résume pas à un simple outil: il s'agit d'un processus entrepris le plus tôt possible dans le cycle d'une initiative, lorsqu'il existe encore des opportunités d'influencer ses résultats et, par là-même, de garantir la protection de la vie privée dès la conception. Ce processus se poursuit jusqu'au déploiement du projet, voire après son déploiement.

Les initiatives varient considérablement en termes d'échelle et d'impact. Les objectifs relevant de la « vie privée » sont fonction de la culture, des attentes sociales et de la juridiction. Le présent document a pour objet de fournir des recommandations adaptables pouvant être appliquées à toute initiative. Étant donné que les recommandations applicables à toutes les circonstances ne peuvent avoir une portée normative, il convient d'interpréter au cas par cas les recommandations données dans le présent document.

Un responsable de traitement de DCP peut avoir la responsabilité de mener un PIA et peut demander à un sous-traitant de DCP de l'assister dans cette tâche, en agissant au nom du responsable de traitement de DCP. Un sous-traitant de DCP ou un fournisseur peut également souhaiter mener son propre PIA.

Les informations de PIA d'un fournisseur sont tout particulièrement pertinentes lorsque le système d'information, l'application ou le processus soumis(e) à évaluation comprend des dispositifs qui utilisent une connexion numérique. Il peut être nécessaire pour des fournisseurs de tels dispositifs de fournir aux personnes chargées de mener le PIA des informations de conception pertinentes du point de vue de la protection de la vie privée. Lorsque le fournisseur de dispositifs numériques ne possède ni les compétences ni les ressources suffisantes pour mener des PIA, par exemple:

— un petit détaillant; ou

— une petite ou moyenne entreprise (PME) utilisant des dispositifs à connexion numérique dans le cadre de ses activités normales,

le fournisseur de dispositifs peut, afin d'être en mesure d'entreprendre une activité PIA de base, être appelé à fournir une grande quantité d'informations relatives à la vie privée et entreprendre son propre PIA en tenant compte de la personne concernée/contexte de PME attendu(e) pour l'équipement qu'il fournit.

Un PIA est généralement mené par un organisme qui prend sa responsabilité au sérieux et qui traite les personnes concernées comme il convient. Dans certaines juridictions, un PIA peut être nécessaire pour satisfaire aux exigences légales et réglementaires.

Le présent document est destiné à être utilisé lorsque l'évaluation des impacts sur la vie privée des personnes concernées inclut la prise en compte de processus, systèmes d'information ou programmes où:

— la responsabilité de la mise en œuvre et/ou de la livraison du processus, du système d'information ou du programme est partagée avec d'autres organismes, et où il convient de veiller à ce que chaque organisme traite les risques identifiés de manière adéquate;

— un organisme gère les risques sur la vie privée dans le cadre de son effort global de management des risques, tout en se préparant à la mise en œuvre ou à l'amélioration de son SMSI (établi conformément à l'ISO/IEC 27001 ou à un système de management équivalent); ou un organisme gère les risques sur la vie privée comme une fonction indépendante;

— un organisme (gouvernemental, par exemple) entreprend une initiative (par exemple, un programme de partenariat public-privé) pour laquelle le futur organisme qui assumera le rôle de responsable

de traitement de DCP n'est pas encore connu, avec comme résultat que le plan de traitement ne peut être directement mis en œuvre et où, par conséquent, il convient que ledit plan de traitement soit plutôt rattaché à la législation, à la réglementation ou au contrat correspondant(e);

— l'organisme souhaite agir de manière responsable vis-à-vis des personnes concernées.

Les mesures jugées nécessaires pour traiter les risques identifiés au cours du processus d'analyse des impacts sur la vie privée peuvent être dérivées de plusieurs ensembles de mesures, notamment l'ISO/IEC 27002 (pour les mesures de sécurité) et l'ISO/IEC 29151 (pour les mesures liées à la protection des DCP) ou de normes nationales comparables, ou peuvent être définies par la personne responsable de la conduite du PIA, indépendamment de tout autre ensemble de mesures.

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'étude d'impacts sur la vie privée

1 Domaine d'application

Le présent document établit des lignes directrices pour:

— un processus d'évaluation des impacts sur la vie privée; et

— une structure et un contenu d'un rapport d'évaluation des impacts sur la vie privée (PIA).

Il s'applique aux organismes de tous types et de toutes tailles, y compris les entreprises publiques et privées, les entités gouvernementales et les organisations à but non lucratif.

Le présent document s'adresse à toute personne impliquée dans la conception ou la réalisation de projets, y compris les parties qui exploitent des systèmes et services de traitement des données qui traitent des DCP.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

Guide ISO 73:2009, *Management du risque — Vocabulaire*

ISO/IEC 27000:2016, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

ISO/IEC 29100:2011, *Technologies de l'information — Techniques de sécurité — Cadre pour la protection de la vie privée*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 29100, l'ISO/IEC 27000 et le Guide ISO 73, ainsi que les suivants, s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— IEC Electropedia: disponible à l'adresse http://www.electropedia.org/

— ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
déclaration d'acceptation
déclaration de management formelle consistant à assumer la responsabilité de la propriété du risque, du traitement du risque et du risque résiduel

3.2
actif
tout ce qui a de la valeur pour quiconque impliqué dans le traitement des données à caractère personnel (DCP)

Note 1 à l'article: Dans le contexte d'un processus de management du risque lié à protection de la vie privée, un actif désigne soit des DCP soit un actif sous-jacent.

3.3
évaluateur
personne qui dirige et conduit une étude d'impacts sur la vie privée (3.7)

Note 1 à l'article: L'évaluateur peut être assisté d'un ou plusieurs autres experts internes/externes intégrés à son équipe.

Note 2 à l'article: L'évaluateur peut être un expert interne ou externe à l'organisme.

3.4
processus
ensemble d'activités corrélées ou en interaction qui transforme des éléments d'entrée en éléments de sortie

[SOURCE: Directives ISO/IEC, Partie 1, Supplément ISO consolidé:2014, 3.12]

3.5
dispositif
combinaison de matériel et de logiciel, ou uniquement de logiciel, permettant à un utilisateur d'exécuter des actions

3.6
impact sur la vie privée
tout ce qui a un effet sur la vie privée d'une personne concernée et/ou d'un groupe de personnes concernées

Note 1 à l'article: L'impact sur la vie privée peut être le résultat du traitement des DCP dans le respect ou en violation des exigences applicables en matière de protection de la vie privée.

3.7
évaluation de l'impact sur la vie privée
PIA
processus global visant à identifier, analyser, évaluer, consulter, communiquer et planifier le traitement des impacts potentiels sur la vie privée au regard du traitement des données à caractère personnel, dans le cadre plus large du système de management des risques d'un organisme

Note 1 à l'article: Adapté de l'ISO/IEC 29100:2011, 2.20.

3.8
carte des risques sur la vie privée
schéma indiquant le niveau d'impact et la probabilité des risques identifiés pour la vie privée

Note 1 à l'article: La carte est généralement utilisée pour déterminer l'ordre dans lequel il convient de traiter les risques sur la vie privée.

3.9
programme
groupe de projets gérés de manière coordonnée afin d'obtenir des bénéfices qu'il ne serait pas possible de produire dans le cadre d'une gestion individuelle

[SOURCE: ISO 14300-1:2011, 3.2, modifiée]

3.10
projet
processus unique qui consiste en un ensemble d'activités coordonnées et maîtrisées comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifiques, incluant les contraintes de délais, de coûts et de ressources

[SOURCE: ISO 9000:2015, 3.4.2]

3.11
organisme
personne ou groupe de personnes ayant un rôle avec les responsabilités, l'autorité et les relations lui permettant d'atteindre ses objectifs

Note 1 à l'article: Le concept d'organisme englobe sans s'y limiter, les travailleurs indépendants, les compagnies, les sociétés, les firmes, les entreprises, les administrations, les partenariats, les organisations caritatives ou les institutions, ou bien une partie ou une combinaison des entités précédentes, à responsabilité limitée ou ayant un autre statut, de droit public ou privé.

[SOURCE: Directives ISO/IEC, Partie 1, Supplément ISO consolidé 2014, 3,01]

3.12
gravité
estimation de l'ampleur des impacts potentiels sur la vie privée d'une personne concernée

3.13
système
système d'information
applications, services, actifs informationnels ou autres composants permettant de gérer l'information

[SOURCE: ISO/IEC 27000:2016, 2.39]

3.14
partie prenante
personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité

Note 1 à l'article: Comprend les personnes concernées, la direction, les organismes de réglementation et les clients.

Note 2 à l'article: La consultation des parties prenantes fait partie intégrante d'un PIA.

[SOURCE: Directives ISO/IEC, Partie 1, Supplément ISO consolidé, 2014, 3.02 – modifiées – Le terme recommandé « partie intéressée » a été supprimé de cet article.]

3.15
technologie
systèmes et éléments de systèmes matériels, logiciels et micrologiciels incluant, sans toutefois s'y limiter, les technologies de l'information, les systèmes intégrés ou tout autre système électromécanique ou reposant sur un processeur

[SOURCE: ISO/IEC 16509:1999, 3.3]

4 Abréviations

API	Interface de programmation d'applications [application programming interface]
AVEC	Apportez votre équipement personnel de communication
DCP	Données à caractère personnel

PME Petites et moyennes entreprises

SMSI Système de management de la sécurité de l'information

TIC Technologies de l'information et de la communication

5 Préparation de la justification d'un PIA

5.1 Avantages de la mise en œuvre d'un PIA

Le présent document fournit des recommandations qui peuvent être adaptées à une grande diversité de situations où sont traitées des DCP. D'une manière générale, cependant, un PIA peut être réalisé en vue:

— d'identifier les impacts sur la vie privée, les risques sur la vie privée et les responsabilités associées;

— de fournir des éléments d'entrée pour la conception d'une protection de la vie privée (parfois appelé « protection de la vie privée dès la conception »);

— d'examiner les risques d'un nouveau système d'information en matière de vie privée, et d'évaluer leur impact et leur probabilité;

— de fournir la base pour la fourniture d'informations sur la vie privée à des personnes concernées concernant toute action d'atténuation recommandée des personnes concernées;

— de conserver les mises à jour ou mises à niveau ultérieures avec des fonctionnalités supplémentaires susceptibles d'impacter les DCP traitées;

— de partager et d'atténuer les risques avec les parties prenantes, ou de fournir des preuves en lien avec la conformité.

NOTE Un PIA est parfois désigné par d'autres termes, par exemple « examen de la protection de la vie privée » ou « évaluation de l'impact de la protection des données ». Ces instances particulières d'un PIA peuvent avoir des implications spécifiques aussi bien sur le plan du processus que sur celui des rapports.

Un PIA a souvent été décrit comme un système d'alerte précoce. Elle offre un moyen de détecter les risques potentiels pour la vie privée qui découlent du traitement des DCP et, ainsi, d'informer un organisme sur les domaines où il convient qu'il prenne des précautions particulières et qu'il développe des moyens de protection adaptés avant (et non pas après) que l'organisme n'engage de lourds investissements. Les coûts liés à la modification d'un projet au stade de la planification représentent en général seulement une fraction des coûts engagés à une phase ultérieure. Si l'impact sur la vie privée est inacceptable, le projet peut même devoir être annulé purement et simplement. Un PIA permet donc d'identifier les problèmes liés à la protection de la vie privée à un stade précoce et/ou de réduire les coûts associés au temps de gestion, aux frais juridiques et aux difficultés publiques ou médiatiques potentielles, en prenant en compte ces problèmes de façon anticipée. Elle peut également aider un organisme à éviter les violations des données à caractère personnel coûteuses ou embarrassantes.

S'il convient qu'un PIA ne se limite pas à une simple vérification de conformité, il n'en reste pas moins qu'il contribue à démontrer la conformité d'un organisme aux exigences applicables en matière de protection de la vie privée et de protection des données en cas de plainte, d'audit sur la protection de la vie privée ou d'enquête de conformité ultérieur(e). Si un risque ou une violation des données à caractère personnel se produit, le rapport de PIA peut apporter la preuve que l'organisme a agi de manière appropriée pour tenter d'empêcher une telle situation. Cela peut aider à réduire, voire à éliminer, toute responsabilité, publicité négative ou atteinte à la réputation.

Un PIA approprié démontre également aux clients et/ou citoyens d'un organisme que celui-ci respecte leur vie privée et est attentif à leurs préoccupations. Les clients ou citoyens ont tendance à faire davantage confiance à un organisme qui entreprend un PIA qu'à un organisme qui n'en fait rien.

Un PIA améliore la prise de décision et met au grand jour les insuffisances au niveau de la communication interne ou les hypothèses cachées sur les questions liées à la protection de la vie privée dans le cadre

du projet. Un PIA est un outil qui permet d'analyser de façon systématique les questions liées à la protection de la vie privée qui découlent d'un projet afin d'en informer les décideurs. Un PIA peut être une source d'informations crédible.

Un PIA permet à un organisme de comprendre immédiatement les insuffisances d'un processus, d'un système d'information ou d'un programme sur le plan de la vie privée, plutôt que de laisser ses auditeurs ou concurrents les pointer du doigt. Un PIA permet d'anticiper les préoccupations du public concernant la protection de la vie privée et d'y répondre.

Un PIA peut aider un organisme à gagner la confiance du public en lui apportant l'assurance que la protection de la vie privée a été intégrée dans la conception d'un processus, d'un système d'information ou d'un programme.

La confiance repose sur la transparence, et un PIA est un processus rigoureux qui encourage des communications ouvertes, une compréhension commune et une transparence. Un organisme qui entreprend un PIA démontre à ses employés et sous-traitants qu'il prend leur vie privée au sérieux et qu'il attend d'eux la même chose en retour. Un PIA est un moyen d'éduquer les employés à la protection de la vie privée et de leur apprendre à être attentifs aux problèmes de protection de la vie privée qui pourraient nuire à l'organisme. C'est un moyen d'affirmer les valeurs de l'organisme. Un PIA peut être utilisé comme une indication de diligence raisonnable et peut réduire le nombre d'audits client.

5.2 Objectifs de la production de rapports de PIA

Les rapports de PIA ont pour but de communiquer les résultats d'évaluation aux parties prenantes. Les diverses parties prenantes ont différentes attentes vis-à-vis d'un PIA.

Des exemples types de parties prenantes et de leurs attentes sont donnés ci-dessous.

— Personne concernée: le PIA est un instrument qui permet aux personnes auxquelles se rapportent les DCP d'avoir l'assurance que leur vie privée est protégée.

— Direction: plusieurs points de vue, à savoir:

  — le PIA considéré comme un instrument permettant de gérer les risques sur la vie privée, de sensibiliser l'opinion et de créer un sens des responsabilités; d'apporter une visibilité sur le traitement des DCP au sein de l'organisme, et sur les éventuels risques et impacts associés; et d'alimenter la stratégie métier ou produit;

  — le développement du PIA dès les premières phases du projet permet de s'assurer que les exigences en matière de protection de la vie privée sont intégrées aux exigences fonctionnelles et non fonctionnelles, qu'elles sont réalisables, viables et traçables par le biais du processus de conduite du changement et de management du risque, et qu'elles peuvent entraîner la suspension ou l'annulation du projet. Il convient que l'effort de classification et de gestion des DCP d'un projet soit comptabilisé dans un poste d'investissement distinct du budget d'un projet ou programme, avec un montant spécifique qui soit acceptable pour l'ensemble des parties prenantes;

  — le PIA considéré comme une opportunité de mieux comprendre les exigences en matière de vie privée et d'évaluer les activités compte tenu de ces exigences; données d'entrée pour la conception et la livraison de produits ou de services; révisée et modifiée dans le cadre du processus de conduite du changement après livraison;

  — le PIA considéré comme un instrument permettant de comprendre les risques liés à la protection de la vie privée au niveau de la fonction/du projet/de l'unité; consolidation des risques; données d'entrée pour les mécanismes de conception et d'application de la politique de protection de la vie privée; données d'entrée pour le redéveloppement des processus de protection de la vie privée.

— Organisme réglementaire: le PIA est un instrument qui contribue à fournir des preuves de conformité aux exigences légales applicables. Il peut apporter une preuve de diligence raisonnable de la part de l'organisme en cas de violation, de non-conformité, de plainte, etc.

— Client: le PIA est un moyen d'évaluer la manière dont le sous-traitant de DCP ou le responsable de traitement de DCP traite les DCP et prouve qu'il respecte ses obligations contractuelles.

Il convient que les rapports de PIA remplissent deux fonctions élémentaires. La première (Inventaire) informe les parties prenantes concernées sur les entités affectées, l'environnement affecté et les risques sur la vie privée identifiés au cours du cycle de vie des entités affectées, qu'ils soient inhérents ou atténués. La deuxième (Éléments d'actions) est un mécanisme de suivi des actions/tâches destinées à améliorer et/ou résoudre les risques sur la vie privée identifiés. Il est nécessaire d'évaluer clairement et de classer (informations privées, confidentielles, publiques, etc.) le caractère sensible de la diffusion et de la publication des informations de rapport.

5.3 Responsabilité de la conduite d'un PIA

Il convient qu'un PIA de processus ou de systèmes d'information soit entrepris par une entité de l'organisme parmi de nombreuses entités différentes, mais un PIA peut également être réalisé sur un processus, un système d'information ou un programme par des associations de consommateurs ou par des organismes non gouvernementaux.

En règle générale, il convient dans un premier temps de confier la responsabilité de s'assurer qu'un PIA est bien effectué à la personne chargée de la protection des DCP et, dans un second temps, au chef de projet qui développe la nouvelle technologie, le nouveau service ou toute autre initiative pouvant affecter la vie privée.

Il convient que la responsabilité de s'assurer que le PIA est bien effectué et de garantir la qualité du résultat (responsabilité du PIA) soit confiée à la direction générale du responsable de traitement de DCP. La personne à qui peut être confiée la responsabilité de conduire le PIA peut le conduire elle-même, peut solliciter l'aide d'autres parties prenantes internes et/ou externes, ou peut faire appel à un tiers indépendant pour effectuer cette tâche en sous-traitance. Chaque approche présente des avantages et des inconvénients.

Cependant, lorsque le PIA est effectué directement par l'organisme, des associations d'utilisateurs ou des instances gouvernementales peuvent demander que l'adéquation du PIA soit vérifiée par un auditeur indépendant.

Il convient que l'organisme veille à ce qu'une responsabilité et une autorité soient établies pour la gestion des risques sur la vie privée, y compris pour la mise en œuvre et la tenue à jour du processus de management des risques sur la vie privée et pour s'assurer de l'adéquation et de l'efficacité de toutes les mesures. Cela peut être facilité par:

— la spécification des responsables de l'élaboration, de la mise en œuvre et de la tenue à jour du cadre organisationnel de management du risque sur la vie privée; et

— la spécification des propriétaires des risques, afin de mettre en œuvre le traitement des risques sur la vie privée, de maintenir les mesures pour la protection de la vie privée et de rendre compte des informations importantes concernant les risques sur la vie privée.

5.4 Échelle d'un PIA

L'échelle du PIA dépendra de l'importance présumée des impacts. Par exemple, s'il est supposé que les impacts affecteront uniquement les employés de l'organisme (par exemple, l'organisme peut souhaiter améliorer son contrôle d'accès par des moyens biométriques, tels qu'une empreinte digitale de chaque employé), alors le PIA peut n'engager que les représentants salariaux et avoir une échelle relativement restreinte. Si, en revanche, un service gouvernemental souhaite introduire un nouveau système de gestion des identités pour l'ensemble des citoyens, il devra organiser un PIA bien plus vaste et impliquant une grande diversité de parties prenantes externes.

Il convient que les organismes effectuent une autoévaluation de l'échelle requise du PIA, conformément aux lois et règlements. La quantité et la granularité des DCP par personne, le degré de sensibilité des DCP, le nombre de personnes concernées et le nombre de personnes ayant accès aux DCP à traiter constituent des facteurs essentiels pour la détermination de cette échelle.

Dans le cas de PME ou d'organismes gouvernementaux ou à but non lucratif, la détermination de l'échelle appropriée du PIA peut être effectuée conjointement, sans que cela soit contraignant, par la personne chargée de conduire un PIA (selon 5.3), par la direction de la PME et/ou avec les conseils d'experts externes si cela est approprié.

6 Recommandations relatives au processus de conduite d'un PIA

6.1 Généralités

Il est nécessaire que le domaine d'application d'un PIA et les détails spécifiques de ce qu'il couvre et de la manière dont il est organisé soient adaptés à la taille de l'organisme, à la juridiction locale et au programme, système d'information ou processus spécifique qui fait l'objet du PIA. Dans l'Article 6 :

— « l'Objectif » est quelque chose qu'il convient d'atteindre;

— les « Éléments d'entrée » fournissent des recommandations sur les informations qui peuvent être nécessaire pour atteindre « l'Objectif »;

— le « Résultat attendu » est la cible « d'Actions » recommandée;

— les « Actions », ou leurs équivalents, sont des recommandations relatives aux activités qu'il peut être nécessaire d'effectuer pour atteindre « l'Objectif » et créer le « Résultat attendu » recommandé; et

— les « Recommandations de mise en œuvre » fournissent davantage de détails sur les sujets qu'il peut être nécessaire de prendre en compte lors de l'exécution des « Actions ».

Dans le présent article, un organisme peut mettre en œuvre de façon indépendante les « Actions », ou leurs équivalents, adaptés au domaine d'application et à l'échelle souhaités d'un PIA. Ces Actions sont conçues pour servir de base raisonnable à la planification, à la mise en œuvre et au suivi du PIA dans diverses circonstances.

L'organisme qui conduit un processus de PIA peut souhaiter adapter directement les recommandations de processus décrites ci-dessous à l'échelle et au domaine d'application spécifiques de sa PIA, de manière à choisir un système de management des risques adapté, tels que l'ISO/IEC 27001, et à y intégrer des éléments de recommandations adaptés comme il convient, y compris l'utilisation du rapport de PIA (voir Article 7) pour traiter les risques sur la vie privée qu'il aura identifiés.

Dans le présent document, le terme « conduire un PIA » est employé pour couvrir aussi bien un PIA initial où les étapes et actions nécessaires sont choisies en réponse à une exigence de PIA particulière, qu'une mise à jour d'un PIA existant où seules sont exécutées les étapes et actions nécessaires dans le cadre de cette mise à jour.

L'Annexe C fournit des recommandations supplémentaires pour faciliter la compréhension des termes utilisés dans le présent document.

Pour aider les PME dans le processus de PIA, il convient d'encourager les associations industrielles ou les organismes de représentation des PME d'élaborer des codes de bonne conduite qui fournissent des lignes directrices pertinentes, et il convient d'encourager les PME à prendre part à ces activités. Des codes de bonne conduite raisonnables doivent normalement respecter les valeurs stipulées dans le présent document et pouvoir être approuvés par les autorités chargées de la protection des données.

6.2 Déterminer si un PIA est nécessaire (analyse du seuil)

Objectif: Déterminer si un nouveau PIA ou si une mise à jour d'un PIA existant est nécessaire.

Élément d'entrée: Informations relatives au programme, au système d'information ou au processus soumis à évaluation.

Résultat attendu: Résultat de l'analyse du seuil, autorisation de préparer un nouveau PIA ou une mise à jour de PIA, le cas échéant, termes de référence et domaine d'application du PIA choisi.

